SIEMENS

SIMATIC NET

Industrial Ethernet Security Nozioni di base e applicazione Security

Manuale di progettazione

Prefazione

Introduzione e nozioni di base 1

Progettazione con Security Configuration Tool 2

Creazione di unità e impostazione dei parametri di rete 3

Progettazione di firewall 4

Progettazione di ulteriori proprietà dell'unità 5

Comunicazione protetta nella VPN tramite tunnel IPsec 6

Ridondanza router e firewall 7

SOFTNET Security Client 8

Funzioni online - Diagnostica e logging 9

Appendice A

Bibliografia B

04/2015

C79000-G8972-C286-05

Avvertenze di legge

Concetto di segnaletica di avvertimento

Questo manuale contiene delle norme di sicurezza che devono essere rispettate per salvaguardare l'incolumità personale e per evitare danni materiali. Le indicazioni da rispettare per garantire la sicurezza personale sono evidenziate da un simbolo a forma di triangolo mentre quelle per evitare danni materiali non sono precedute dal triangolo. Gli avvisi di pericolo sono rappresentati come segue e segnalano in ordine descrescente i diversi livelli di rischio.

⚠PERICOLO
questo simbolo indica che la mancata osservanza delle opportune misure di sicurezza **provoca** la morte o gravi lesioni fisiche.

⚠AVVERTENZA
il simbolo indica che la mancata osservanza delle relative misure di sicurezza **può causare** la morte o gravi lesioni fisiche.

⚠CAUTELA
indica che la mancata osservanza delle relative misure di sicurezza può causare lesioni fisiche non gravi.

ATTENZIONE
indica che la mancata osservanza delle relative misure di sicurezza può causare danni materiali.

Nel caso in cui ci siano più livelli di rischio l'avviso di pericolo segnala sempre quello più elevato. Se in un avviso di pericolo si richiama l'attenzione con il triangolo sul rischio di lesioni alle persone, può anche essere contemporaneamente segnalato il rischio di possibili danni materiali.

Personale qualificato

Il prodotto/sistema oggetto di questa documentazione può essere adoperato solo da **personale qualificato** per il rispettivo compito assegnato nel rispetto della documentazione relativa al compito, specialmente delle avvertenze di sicurezza e delle precauzioni in essa contenute. Il personale qualificato, in virtù della sua formazione ed esperienza, è in grado di riconoscere i rischi legati all'impiego di questi prodotti/sistemi e di evitare possibili pericoli.

Uso conforme alle prescrizioni di prodotti Siemens

Si prega di tener presente quanto segue:

⚠AVVERTENZA
I prodotti Siemens devono essere utilizzati solo per i casi d’impiego previsti nel catalogo e nella rispettiva documentazione tecnica. Qualora vengano impiegati prodotti o componenti di terzi, questi devono essere consigliati oppure approvati da Siemens. Il funzionamento corretto e sicuro dei prodotti presuppone un trasporto, un magazzinaggio, un’installazione, un montaggio, una messa in servizio, un utilizzo e una manutenzione appropriati e a regola d’arte. Devono essere rispettate le condizioni ambientali consentite. Devono essere osservate le avvertenze contenute nella rispettiva documentazione.

Marchio di prodotto

Tutti i nomi di prodotto contrassegnati con ® sono marchi registrati della Siemens AG. Gli altri nomi di prodotto citati in questo manuale possono essere dei marchi il cui utilizzo da parte di terzi per i propri scopi può violare i diritti dei proprietari.

Esclusione di responsabilità

Abbiamo controllato che il contenuto di questa documentazione corrisponda all'hardware e al software descritti. Non potendo comunque escludere eventuali differenze, non possiamo garantire una concordanza perfetta. Il contenuto di questa documentazione viene tuttavia verificato periodicamente e le eventuali correzioni o modifiche vengono inserite nelle successive edizioni.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANIA

N. di ordinazione documentazione: C79000-G8972-C286-05
℗ 05/2015 Con riserva di modifiche

Copyright © Siemens AG 2012 - 2015.
Tutti i diritti riservati

Prefazione

Prefazione

Questo manuale...

…fornisce un supporto durante la progettazione delle funzionalità Security dei seguenti prodotti "Security Integrated":

- SCALANCE S: S602 / S612 / S623 / S627-2M
- SOFTNET Security Client
- CP S7: CP 343-1 Advanced, CP 443-1 Advanced
- CP PC: CP 1628
- Router rete mobile: SCALANCE M875
- SCALANCE M-800:
  - Router ADSL: SCALANCE M81x
  - Router SHDSL: SCALANCE M82x
  - Router rete mobile: SCALANCE M874-2 nonché SCALANCE M874-3

Denominazione generale "Unità Security"

Nella seguente documentazione i seguenti prodotti vengono aggruppati nella denominazione "Unità Security": SCALANCE S602 / SCALANCE S612 / SCALANCE S623 / SCALANCE S627-2M, CP 343-1 Advanced, CP 443-1 Advanced, CP 1628.

Le differenze delle funzioni vengono contrassegnate con simboli (vedere sezione "Spiegazione dei simboli"). Le descrizioni dell'hardware e le avvertenze per l'installazione si trovano nelle documentazioni delle singole unità.

Utilizzo delle denominazioni "Interfaccia" e "Porta"

Nella presente documentazione vengono utilizzate le seguenti denominazioni per le porte delle unità SCALANCE S:

- "Interfaccia esterna": La porta esterna in SCALANCE S602 / S612 / S623 o una porta esterna in SCALANCE S627-2M (contrassegno rosso)
- "Interfaccia interna": La porta interna in SCALANCE S602 / S612 / S623 o una porta interna in SCALANCE S627-2M (contrassegno verde)
- "Interfaccia DMZ": La porta DMZ in SCALANCE S623 / S627-2M (contrassegno giallo)

La denominazione "Porta" stessa viene quindi utilizzata se una porta specifica di un'interfaccia ha la priorità.

Denominazione generale "STEP 7"

La progettazione delle funzioni Security dei CP è possibile a partire da STEP 7 V5.5 SP2 HF1. Per questo motivo nella presente documentazione viene utilizzata la denominazione "STEP 7" al posto delle versioni di STEP 7 a partire da V5.5 SP2 HF1 fino alla versione inferiore di STEP 7 V10. La progettazione delle funzioni Security di tutte le unità Security in STEP 7 a partire dalla V12 è descritta nel sistema informativo in STEP 7 a partire dalla V12, sezione "Industrial Ethernet Security".

Denominazione generale "CP x43-1 Adv."

Nella seguente documentazione i seguenti prodotti vengono raggruppati nella denominazione "CP x43-1 Adv.": CP 343-1 Advanced / CP 443-1 Advanced.

Security Configuration Tool V4.1 - Nuove funzioni

Con il Security Configuration Tool V4.1 sono considerate le seguenti nuove funzioni:

- **Estensione della funzionalità VPN per le unità SCALANCE M**

  È supportata la realizzazione attiva del collegamento VPN da un'unità SCALANCE M ad un'unità SCALANCE M-800.

- **Estensione della funzionalità "Ridondanza del router e del firewall" per unità SCALANCE S623/S627-2M a partire dal firmware V4.0.1**

  La progettazione di ID del router virtuali per le interfacce virtuali delle relazioni di ridondanza è supportata per le unità SCALANCE S623/S627-2M a partire dal firmware V4.0.1.

- **Estensione della funzionalità firewall per unità SCALANCE S a partire dal firmware V3**

  La progettazione di regole IP senza States firewall è supportata solo per unità SCALANCE S a partire dal firmware V3.

Campo di validità di questo manuale

Questo manuale è valido per le seguenti unità SIMATIC NET:

Unità	MLFB
SCALANCE S602	6GK5 602-0BA10-2AA3
SCALANCE S612	6GK5 612-0BA10-2AA3
SCALANCE S623	6GK5 623-0BA10-2AA3
SCALANCE S627-2M	6GK5 627-2BA10-2AA3
CP 343-1 Advanced a partire da V3	6GK7 343-1GX31-0XE0
CP 443-1 Advanced a partire da V3	6GK7 443-1GX30-0XE0
CP 1628	6GK1162-8AA00

Questo manuale è valido per i seguenti strumenti di progettazione SIMATIC NET:

Strumento di progettazione	MLFB	Versione
SOFTNET Security Client	6GK1704-1VW05-0AA0	V5.0
Security Configuration Tool (SCT)	-	V4.1

Destinatari

Il presente manuale è rivolto a persone che configurano le funzionalità Industrial Ethernet Security in una rete.

SIMATIC NET Manual Collection (n. di orinazione A5E00069051)

Alle unità SCALANCE S, al CP S7 e al CP PC 1628 è allegato la SIMATIC NET Manual Collection. Questa Manual Collection viene aggiornata regolarmente e contiene i manuali e le descrizioni attuali al momento della creazione.

Marchi

Le seguenti denominazioni o eventuali altre denominazione non contrassegnate con il marchio relativo alla proprietà esclusiva ® sono marchi registrati di Siemens AG:

C-PLUG, CP 343-1, CP 443-1, SCALANCE, SIMATIC, SOFTNET

Simboli ricorrenti in queste istruzioni

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per SCALANCE S a partire da V3.0.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per SCALANCE S a partire da V4.0.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per SCALANCE S.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per SCALANCE M.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante per tutte le unità tranne SCALANCE M875.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante per tutte le unità tranne SCALANCE M.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante per tutte le unità Security tranne SCALANCE S602.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante per tutte le unità Security tranne S < V3.0.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per SCALANCE S602 a partire da V3.1.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per SCALANCE S623.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per SCALANCE S627-2M.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per SCALANCE S623 e SCALANCE S627-2M.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per SCALANCE S623 a partire da V4.0 e SCALANCE S627-2M a partire da V4.0.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per CP S7.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante per tutte le unità Security tranne i CP S7.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante solo per CP PC.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante per tutte le unità Security tranne i CP PC.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante per tutti i CP S7 e i CP PC.

Il capitolo descritto / la sezione descritta / la riga descritta è rilevante per tutte le unità Security tranne i CP.

Il simbolo rimanda ad una particolare bibliografia raccomandata.

Questo simbolo rimanda ad una guida dettagliata nella guida in base al contesto. Alla guida è possibile accedere con il tasto F1 o con il pulsante "Help" nella relativa finestra di dialogo.

Rimandi bibliografici /.../

I rimandi ad ulteriori documentazioni sono indicati con un numero bibliografico riportato tra due barre /.../. In base a questi numeri è possibile rilevare dalla bibliografia riportata alla fine del presente manuale la parte di documentazione.

Vedere anche

Pagine Customer Support
(http://support.automation.siemens.com/WW/view/it/18701555/130000)

Glossario SIMATIC NET

Descrizione dei numerosi termini specifici, presenti nella documentazione che si trovano nel glossario SIMATIC NET.

Il glossario SIMATIC NET si trova:

- SIMATIC NET Manual Collection o DVD del prodotto

  Il DVD è allegato ad alcuni prodotti SIMATIC NET.
- In Internet alla seguente ID articolo:

  50305045 (http://support.automation.siemens.com/WW/view/it/50305045)

Indice del contenuto

Prefazione 3

1 Introduzione e nozioni di base 15

1.1 Avvertenze importanti 15

1.2 Introduzione e nozioni di base 18

1.3 Proprietà del prodotto 18
1.3.1 Panoramica delle funzioni 18
1.3.2 Strutture d'insieme 20
1.3.3 Regole per nome utente, ruoli e password 21
1.3.4 Sostituzione dell'unità 23

1.4 Impiego del SOFTNET Security Client 24

1.5 Impiego di SCALANCE S602 25

1.6 Impiego di SCALANCE S612, S623 e S627-2M 28

1.7 Impiego dell'interfaccia DMZ di SCALANCE S623 e SCALANCE S627-2M 31

1.8 Impiego delle porte dei modulo mediali di SCALANCE S627-2M 35

1.9 Impiego di CP 343-1 Advanced e CP 443-1 Advanced 36

1.10 Impiego del CP 1628 38

1.11 Progettazione e amministrazione 40

2 Progettazione con Security Configuration Tool 41

2.1 Panoramica - Potenzialità e tipi di funzionamento 41

2.2 Installazione del Security Configuration Tool 43
2.2.1 Sistemi operativi supportati 43

2.3 Superficie operativa e voci di menu 45

2.4 Creazione e gestione di progetti 51
2.4.1 Security Configuration Tool (variante standalone) 51
2.4.2 Security Configuration Tool in STEP 7 51
2.4.3 Migrazione di dati STEP 7 55
2.4.4 Informazioni generali 56
2.4.5 Definizione dei valori di inizializzazione standard per un progetto 60
2.4.6 Controlli di coerenza 61
2.4.7 Impostazione di nomi simbolici per indirizzi IP/MAC. 62

2.5 Gestione degli utenti 64
2.5.1 Panoramica della gestione utenti 64
2.5.2 Crea utente 66
2.5.3 Creazione dei ruoli 67
2.5.4 Gestione dei diritti 69
2.5.5 Progettazione delle direttive password 73
2.5.6 Autenticazione mediante server RADIUS 75

2.5.6.1 Informazioni generali ... 75
2.5.6.2 Definizione del server ADIUS ... 78
2.5.6.3 Assegnazione del server RADIUS ad un'unità Security ... 79

2.6 Gestione dei certificati ... 80
2.6.1 Informazioni generali ... 80
2.6.2 Rinnovo dei certificati ... 82
2.6.3 Sostituzione di certificati ... 84

3 Creazione di unità e impostazione dei parametri di rete ... 85

3.1 Parametri nell'area del contenuto ... 88

3.2 Configurazione delle interfacce ... 90
3.2.1 Panoramica delle possibilità di collegamento ... 90
3.2.2 Interfacce ... 94
3.2.3 Collegamento Internet ... 98
3.2.4 DNS dinamico (DDNS) ... 99
3.2.5 LLDP ... 101
3.2.6 Ridondanza del mezzo nelle topologie ad anello ... 102
3.2.6.1 Ridondanza del mezzo con MRP/HRP ... 102
3.2.6.2 Progettazione MRP/HRP per le unità Security ... 103
3.2.7 Particolarità della modalità Ghost ... 105

4 Progettazione di firewall ... 111

4.1 CP in modalità standard ... 113
4.1.1 CP x43-1-Adv. ... 114
4.1.1.1 Preimpostazione del firewall ... 114
4.1.1.2 Progettazione di firewall ... 116
4.1.1.3 Progettazione dell'elenco degli accessi ... 117
4.1.1.4 Aggiunta di una voce nell'elenco di accesso ... 119
4.1.2 CP 1628 ... 119
4.1.2.1 Preimpostazione del firewall ... 119
4.1.2.2 Progettazione di firewall ... 122

4.2 SCALANCE S in modalità standard ... 124
4.2.1 Preimpostazione del firewall ... 124
4.2.2 Progettazione del firewall per SCALANCE S ≥ V3.0 ... 129
4.2.3 Progettazione del firewall per SCALANCE S < V3.0 ... 132

4.3 Firewall in modalità estesa ... 134
4.3.1 Progettazione del firewall in modalità estesa ... 134
4.3.2 Set di regole firewall globali ... 135
4.3.2.1 Set di regole firewall globali - Accordi ... 137
4.3.2.2 Creazione e assegnazione di set di regole firewall globali ... 137
4.3.3 Set di regole IP specifiche per l'utente ... 138
4.3.3.1 Creazione e assegnazione di set di regole IP personalizzati ... 139
4.3.4 Regole firewall automaticamente riferite al collegamento ... 141
4.3.5 Impostazione delle regole del filtro pacchetto IP locali ... 144
4.3.6 Regole del filtro pacchetto IP ... 145
4.3.7 definizione dei servizi IP ... 152
4.3.8 definizione dei servizi ICMP ... 153
4.3.9 Impostazione di regole del filtro pacchetto MAC ... 154
4.3.10 Regole del filtro pacchetto MAC ... 155
4.3.11 definizione dei servizi MAC ... 157

4.3.12 configurazione di gruppi di servizi....160
4.3.13 Adattamento delle regole standard per servizi IP....160

5 Progettazione di ulteriori proprietà dell'unità....163

5.1 Unità Security come router....163
5.1.1 Informazioni generali....163
5.1.2 Definizione del router standard e degli instradamenti....164
5.1.3 Routing NAT/NAPT....165
5.1.4 Conversione di indirizzi NAT/NAPT....168
5.1.5 Conversione di indirizzi con tunnel NAT/NAPT nei tunnel VPN....174
5.1.6 Relazione tra router NAT/NAPT e firewall....175
5.1.7 Relazione tra router NAT/NAPT e firewall specifico per l'utente....178
5.2 Unità Security come server DHCP....180
5.2.1 Informazioni generali....180
5.2.2 Configurazione del server DHCP....181
5.3 Sincronizzazione dell'ora....185
5.3.1 Informazioni generali....185
5.3.2 Configurazione della gestione dell'ora....186
5.3.3 Definire il server NTP....187
5.4 SNMP....188
5.4.1 Informazioni generali....188
5.4.2 Attiva SNMP....189
5.5 Proxy ARP....190

6 Comunicazione protetta nella VPN tramite tunnel IPsec....191

6.1 VPN con unità Security e SCALANCE M....191
6.2 Metodo di autenticazione....194
6.3 Gruppi VPN....195
6.3.1 Regole per la formazione di gruppi VPN....195
6.3.2 Rapporti di comunicazione via tunnel supportati....196
6.3.3 Creazione di gruppi VPN e assegnazione e assegnazione di unità....197
6.4 Configurazione del tunnel nella modalità Standard....199
6.5 Configurazione del tunnel in modalità estesa....199
6.5.1 Progettazione delle proprietà del gruppo VPN....200
6.5.2 Acquisizione dell'unità nel gruppo VPN configurato....202
6.5.3 Progettazione delle proprietà VPN specifiche per l'unità....205
6.5.4 Progettazione delle proprietà VPN specifiche per il collegamento....208
6.6 Dati di configurazione per le unità SCALANCE M....210
6.7 Dati di configurazione per apparecchi VPN....213
6.8 Dati di configurazione per NCP VPN Client (Android)....215
6.9 Configurazione di nodi di rete interni....217
6.9.1 Configurazione di ulteriori nodi e sottoreti per il tunnel VPN....217
6.9.2 Tipo di funzionamento della modalità di programmazione....219
6.9.3 Visualizzazione dei nodi di rete interni trovati....221

7 Ridondanza router e firewall....223

7.1 Informazioni generali ... 223
7.2 Relazioni di ridondanza e assegnazione di unità Security ... 224
7.3 Configurazione delle relazioni di ridondanza ... 225
8 SOFTNET Security Client ... 227
8.1 Impiego del SOFTNET Security Client ... 227
8.2 Installazione del SOFTNET Security Client ... 230
8.2.1 Installazione del SOFTNET Security Client ... 230
8.2.2 Disinstallazione del SOFTNET Security Client ... 230
8.3 Impostazione dei file di configurazione con lo strumento di progettazione Security Configuration Tool ... 230
8.4 Finestra di dialogo principale del SOFTNET Security Client ... 233
8.5 Caricamento del file di configurazione e configurazione dei collegamenti via tunnel ... 235
8.6 Diagnostica e configurazione del tunnel - finestra di dialogo "Tunnel Overview" ... 236
8.7 Creazione della configurazione gestita - Finestra di dialogo "Manage users and groups" ... 239
8.8 Esecuzione della diagnostica estesa - finestra di dialogo "Extended Diagnostics" ... 241
8.9 Accesso ai file Log - finestra di dialogo "Log files" ... 242
8.10 Attivazione di regole firewall Windows - finestra di dialogo "Windows firewall parameter assignment" ... 243
8.11 Impostazioni SOFTNET Security Client - finestra di dialogo "Settings" ... 245
9 Funzioni online - Diagnostica e logging ... 249
9.1 Panoramica delle funzioni della finestra di dialogo online ... 251
9.2 Registrazione di eventi (logging) ... 253
9.2.1 Logging locale - Impostazioni nella configurazione ... 255
9.2.2 Network Syslog - Impostazioni nella configurazione ... 257
9.2.3 Progettazione del logging pacchetti ... 260
A Appendice ... 263
A.1 Conformità DNS ... 263
A.2 Aree dei valori indirizzo IP, maschera della sottorete indirizzo dell'accoppiamento ad altra rete ... 263
A.3 MAC adress ... 264
B Bibliografia ... 267
B.1 Introduzione - senza CD/DVD ... 267
B.2 CP S7 / Per la progettazione, la messa in servizio e l'utilizzo del CP ... 268
B.3 Per la progettazione con STEP 7 / NCM S7 ... 268
B.4 CP S7 Per il montaggio e la messa in servizio del CP ... 269
B.5 Per la configurazione e il funzionamento di una rete Industrial Ethernet ... 270
B.6 Nozioni di base SIMATIC e STEP 7 ... 270

B.7 Comunicazione industriale volume 2 271
B.8 Per la configurazione di stazioni PC / PG 271
B.9 Per la configurazione CP PC 271
B.10 SIMATIC NET Industrial Ethernet Security 272
Indice analitico 273

Introduzione e nozioni di base

1

Indicazioni di sicurezza

Siemens commercializza prodotti di automazione e di azionamento per la sicurezza industriale che contribuiscono al funzionamento sicuro di impianti, soluzioni, macchinari, apparecchiature e/o reti. Questi prodotti sono componenti essenziali di una concezione globale di sicurezza industriale. In quest'ottica i prodotti Siemens sono sottoposti ad un processo continuo di sviluppo. Consigliamo pertanto di controllare regolarmente la disponibilità di aggiornamenti relativi ai prodotti.

Per il funzionamento sicuro di prodotti e soluzioni Siemens è necessario adottare idonee misure preventive (ad es. un concetto di protezione di cella) e integrare ogni componente in un concetto di sicurezza industriale globale all'avanguardia. In questo senso si devono considerare anche gli eventuali prodotti impiegati di altri costruttori. Per ulteriori informazioni sulla sicurezza industriale, vedere http://www.siemens.com/industrialsecurity.

Per restare informati sugli aggiornamenti cui vengono sottoposti i nostri prodotti, suggeriamo di iscriversi ad una newsletter specifica del prodotto. Per ulteriori informazioni, vedere http://support.automation.siemens.com.

1.1 Avvertenze importanti

Generale

Nota

Protezione da accesso non autorizzato

Fare attenzione che il computer di progettazione (PC/PG) o il progetto siano protetti da accesso non autorizzato.

Nota

Disattivazione dell'account ospite

Assicurarsi che l'account ospite sul computer di progettazione sia disattivato.

Nota

Data attuale e ora attuale sulle unità Security

In caso di utilizzo di comunicazione protetta (ad es. HTTPS, VPN...) fare attenzione che le unità Security interessate dispongano dell'ora e della data attuale. I certificati utilizzati vengono altrimenti valutati non validi e la comunicazione protetta non funziona.

Nota

Software antivirus attuali

Si raccomanda di installare e aggiornare sempre un software antivirus attuale su tutti i computer di progettazione.

Nota

FTPS

Se nella presente documentazione viene utilizzata la denominazione "FTPS", si intende FTPS in modalità esplicita (FTPES).

Nota

Non è possibile una ricommutazione alla modalità standard

Una commutazione nella modalità estesa per il progetto attuale non può più essere annullata.

Rimedio per SCT Standalone: Chiudere il progetto senza salvarlo e aprirlo di nuovo.

Nota

Misure Security supplementari in caso di utilizzo del SOFTNET Security Client

Il SOFTNET Security Client offre una soluzione per la comunicazione sicura con le celle di automazione tramite VPN. Per una protezione intrinseca del PC/PG nonché della cellula di automazione collegata si raccomanda di impiegare misure supplementari quali ad es. programmi antivirus e firewall Windows.

In Windows 7 il firewall del sistema operativo deve sempre essere attivo in modo che funzioni la realizzazione del tunnel VPN.

CP x43-1 Adv.

Nota

Impostazioni di sicurezza supplementari

Per impedire che dati di progettazione non autorizzati vengano caricati nel CP, è necessario effettuare impostazioni di sicurezza supplementari sul firewall del CP (ad es. della comunicazione S7 o autorizzazione della comunicazione solo via tunnel) o adottare misure di sicurezza esterne.

STEP 7

Nota

"Salva e compila" dopo le modifiche

Per consentire che le impostazioni Security vengano acquisite nei blocchi di sistema (offline) corrispondenti, dopo aver eseguire le modifiche selezionare il menu "Stazione" > "Salva e compila" nella configurazione HW o "Rete" > "Salva e compila" in NetPro.

Nota

Apertura di una stazione con il Security Configuration Tool aperto

Chiudere il Security Configuration Tool prima di aprire un'altra stazione tramite il SIMATIC Manager o NetPro.

Nota

Nessun multiprogetto STEP 7 in combinazione con Security

Per ciascun progetto STEP 7 durante l'attivazione di Security viene creata una configurazione Security univoca. Per questi motivo i multiprogetti STEP 7 non sono supportati in combinazione con Security.

1.2 Introduzione e nozioni di base

Le unità SIMATIC NET Security e il SIMATIC NET SOFTNET Security Client rappresentano il concetto di sicurezza SIEMENS, mirato a soddisfare le richieste di sicurezza di comunicazione nella tecnica di automazione industriale.

Nota

Software antivirus attuali

Si raccomanda di installare sempre un software antivirus attuale su tutti i computer di progettazione.

Questo capitolo fornisce informazioni generali sulle funzioni di sicurezza degli apparecchi e dei componenti:

- SCALANCE S
- CP x43-1 Adv.
- CP 1628
- SOFTNET Security Client

Suggerimento:

Per poter utilizzare rapidamente le unità Security consultare la documentazione "SIMATIC NET Security - Getting Started".

1.3 Proprietà del prodotto

1.3.1 Panoramica delle funzioni

Panoramica delle funzioni dei tipi di unità

Rilevare dalla seguente tabella le funzioni supportate dalle singole unità Security.

Nota

In questo manuale vengono descritte tutte le funzioni. In base alla seguente tabella osservare le funzioni che riguardano le unità Security utilizzate.

Fare attenzione anche alle indicazioni supplementari nei titoli dei capitoli!

Tabella 1- 1 Panoramica delle funzioni

Funzionamento	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V4.0
Progettazione tramite			
Security Configuration Tool	-	-	x
Security Configuration Tool integrato in STEP 7	x	x	x
Compatibilità con elenchi IP Access Control (ACL)	x	-	-
Generale			
Router NAT/NAPT	x	-	x
Routing NAT/NAPT nei collegamenti VPN	-	-	x S602
Server DHCP	-	-	x
Firewall			
Regole firewall locali	x	x	x
Set di regole firewall globali	x	x	x
Set di regole IP specifiche per l'utente	-	-	x
IPsec			
Realizzazione di tunnel IPsec	x	x	x S602
Gestione utenti			
Gestione utenti	x	x	x
Migrazione della gestione attuale degli utenti	x	-	x
Autenticazione utente mediante server RADIUS	-	-	x
Protocollo supportati			
SNMPv3	x	x	x
Server HTTPS	x	-	x
Server FTPS	x	-	-
Client FTPS	x	-	-
Client NTP	x	x	x
Client NTP (protetto)	x	x	x
Client PPPoE	-	-	x
Client DDNS / client DNS	-	-	x
LLDP	x	-	x
Client MRP/HRP	-	-	x S627-2M
Logging			
Registrazione di eventi di sistema	x	x	x
Registrazione di eventi Audit	x	x	x
Registrazione di eventi filtro pacchetto	x	x	x

Funzionamento	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V4.0
Messaggi Audit nei buffer di diagnostica dell'unità Security	x	x	-
Accesso tramite Security Configuration Tool al buffer Log dell'unità Security	x	x	x
Diagnostica tramite Security Configuration Tool	x	x	x
Invio di messaggi al server Syslog	x	x	x
Diagnostica Web	x	-	-
Modalità Ghost			
Rilevamento dell'indirizzo IP di un nodo interno durante l'esecuzione e acquisizione dell'indirizzo IP per la porta esterna dell'unità Security.	-	-	x S602 ≥V3.1
Zona demilitarizzata (DMZ)			
Configurazione di una DMZ per il disaccoppiamento della rete sicura dalla rete non sicura	-	-	x S62x
Ridondanza router e firewall			
Versione ridondante delle unità Security per ottenere la funzionalità router e firewall in caso di guasto di unità Security	-	-	x S62x ≥ V4.0

x La funzione è supportata

- La funzione non è supportata

1.3.2 Strutture d'insieme

Nota

Una panoramica competa delle strutture d'insieme ammesse si trovano in Internet al seguente indirizzo: (http://support.automation.siemens.com/WW/view/it/58217657).

Strutture d'insieme

Funzionamento	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V4.0
Tunnel VPN per ciascuna unità Security	max. 32	max. 64	max. 128 ~~S602~~
Regole firewall per ciascuna unità Security	max. 256		
Server NTP creabili per tutto il progetto (server NTP assegnabili per ciascuna unità Security)	32 (4)		

1.3.3 Regole per nome utente, ruoli e password

Quali regole valgono per il nome utente, il nome di ruolo e le password?

Durante la creazione o la modifica di un utente, un ruolo o una password osservare le seguenti regole:

Caratteri ammessi	Sono consentiti i seguenti caratteri del set di caratteri ANSI X 3.4-1986: 0123456789 A...Z a...z !#$%&()*+,-./:;<=>?@ [\]_{|}~^
Caratteri non consentiti	" ' ` §
Lunghezza del nome utente (metodo di autenticazione "Password")	1 ... 32 caratteri
Lunghezza del nome utente (metodo di autenticazione "RADIUS")	1 ... 255 caratteri
Lunghezza della password	8 ... 32 caratteri
Lunghezza del nome del ruolo	1 ... 32 caratteri
Numero massimo di utenti per ogni progetto	128
Numero massimo di utenti su un'unità Security	32 + 1 amministratore per la creazione del progetto
Numero massimo di ruoli per ogni progetto	128 (122 ruoli definiti dall'utente + 6 ruoli definiti dal sistema)
Numero massimo di ruoli su un'unità Security	37 (31 ruoli definiti dall'utente + 6 ruoli definiti dal sistema)

Nota

Nomi utente e password

Come misura più importate per aumentare la sicurezza prestare attenzione che i nomi utente e le password siano sufficientemente lunghi e che contengano caratteri speciali, caratteri maiuscoli/minuscoli e cifre.

Con le direttive delle password è possibile limitare ulteriormente le restrizioni riportate sopra per le password. La definizione delle direttive per le password sono descritte nel capitolo: Progettazione delle direttive password (Pagina 73)

Complessità password

Durante l'inserimento di una nuova password ne viene controllata la complessità. Per la complessità password si distinguono i seguenti livelli:

- poco complessa
- non complessa
- mediamente complessa

- sufficientemente complessa
- complessa
- molto complessa

Nota

Controllo della complessità password di utenti già esistenti

Verificare la complessità password

- di utenti già esistenti nel progetto,
- del primo utente creato in STEP 7,
- di utenti migrati,

Selezionando il rispettivo utente nella scheda "Utenti" della gestione utenti e facendo clic sul pulsante "Modifica...".

1.3.4 Sostituzione dell'unità

A questa funzione si accede nel modo seguente

1. Selezionare l'unità Security da modificare o il client SOFTNET Security da modificare.
2. Selezionare la voce di menu "Modifica" > "Sostituisci unità...".
3. In base al tipo di prodotto del prodotto e al release del firmware dell'unità selezionata è possibile adattare il tipo di unità e/o il release del firmware nella finestra di dialogo.

Rilevare dalla seguente tabella quali unità possono essere sostituite senza o con eventuale perdita dei dati.

Nota

Sostituzione di CP

Le informazioni relative alla sostituzione di CP si trovano nel rispettivo manuale.

Unità di uscita	Possibile sostituzione dell'unità											
	S602 V2	S602 V3	S602 V4	S612 V1	S612 V2	S612 V3	S612 V4	S613 V1	S613 V2	S623 V3	S623 V4	S627-2M V4
S602 V2	-	x	x	!	x	x	x	!	x	x	x	x
S602 V3	!	-	x	!	!	!	!	!	!	!	!	!
S602 V4	!	!	-	!	!	!	!	!	!	!	!	!
S612 V1	!	!	!	-	x	x	x	x	x	x	x	x
S612 V2	!	!	!	!	-	x	x	!	x	x	x	x
S612 V3	!	!	!	!	!	-	x	!	!	x	x	x
S612 V4	!	!	!	!	!	!	-	!	!	x	x	x
S613 V1	!	!	!	!	!	x	x	-	x	x	x	x
S613 V2	!	!	!	!	!	x	x	!	-	x	x	x
S623 V3	!	!	!	!	!	!	!	!	!	-	x	x
S623 V4	!	!	!	!	!	!	!	!	!	!	-	x
S627-2M V4	!	!	!	!	!	!	!	!	!	!	!	-

x senza perdite

! con eventuali perdite

- Il tipo di unità e la versione firmware non vengono modificati.

Configurazione iniziale	Possibile sostituzione			
	SOFTNET Security Client 2005	SOFTNET Security Client 2008	SOFTNET Security Client V3.0	SOFTNET Security Client V4.0
SOFTNET Security Client 2005	-	x	x	x
SOFTNET Security Client 2008	x*	-	x	x
SOFTNET Security Client V3.0	x* **	x**	-	x
SOFTNET Security Client V4.0	x* **	x**	x	-

***** Se il client SOFTNET Security non si trova in un gruppo routing.

****** Se il SOFTNET Security Client non si trova in un gruppo VPN con un'unità SCALANCE M.

Vedere anche

Superficie operativa e voci di menu (Pagina 45)

/2/ (Pagina 268)

1.4 Impiego del SOFTNET Security Client

Comunicazione PG/PC in VPN - Compito del SOFTNET Security Client

Con il software PC SOFTNET Security Client sono possibili accessi remoti sicuri dal PG/PC agli apparecchi di automazione protetti da unità Security, in tutte le reti pubbliche.

Con il SOFTNET Security Client un PG/PC viene configurato automaticamente in modo che esso possa realizzare una comunicazione sicura tramite tunnel IPsec nella VPN (Virtual Private Network) con una o diverse unità Security.

Le applicazioni PG/PC come la diagnostica NCM o STEP7 possono accedere con un collegamento via tunnel protetto a dispositivi o reti che si trovano in una rete interna protetta con unità Security.

Anche il software PC SOFTNET Security Client viene configurato con lo strumento di progettazione Security Configuration Tool; in questo modo viene garantita la progettazione completamente integrata.

1.5 Impiego di SCALANCE S602

Firewall e Router - Compito di SCALANCE S602

Grazie alla combinazione di diverse misure di sicurezza, quali firewall e router NAT/NAPT, l'unità SCALANCE S602 protegge singoli dispositivi o intere celle di automazione da:

- spionaggio dei dati
- accessi indesiderati

SCALANCE S602 consente questa protezione in modo flessibile e senza trattamenti complessi.

SCALANCE S602 viene configurato con lo strumento di progettazione Security Configuration Tool.

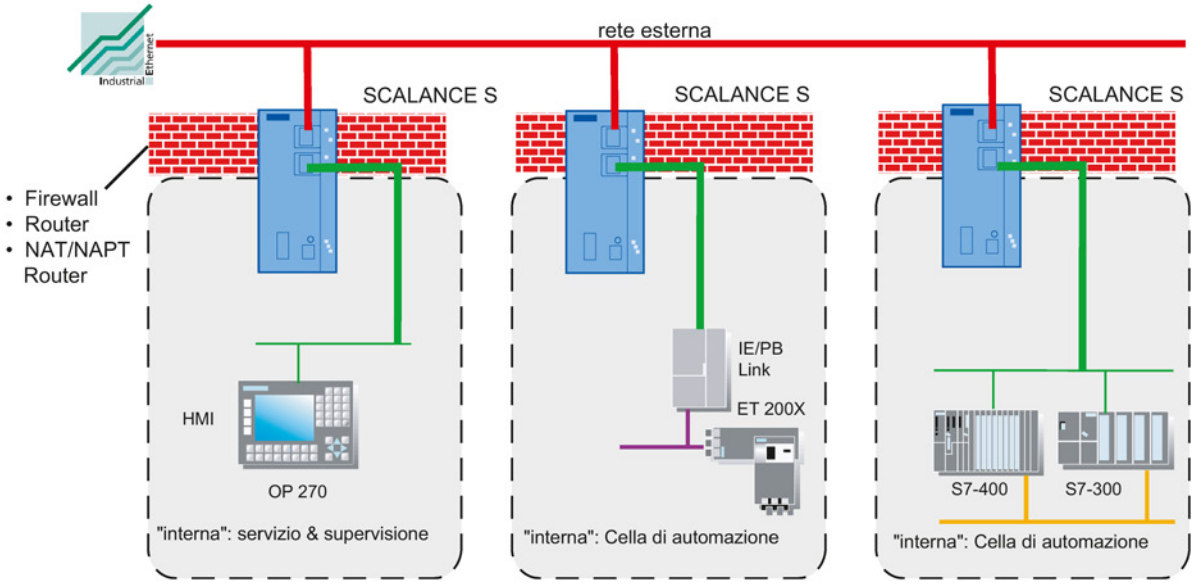


Figura 1-1 Configurazione della rete con SCALANCE S602

Funzioni di sicurezza

- Firewall
  - IP Firewall con Stateful Packet Inspection (layer 3 e 4)
  - Firewall anche per telegrammi Ethernet-"Non-IP" secondo IEEE 802.3

    (telegrammi layer 2; non vale per S602, se viene utilizzato il funzionamento router);
  - Limitazione della larghezza di banda
  - Set di regole firewall globali
  - Set di regole IP specifiche per l'utente

  Tutti i nodi di rete che si trovano in un segmento di rete interno di uno SCALANCE S sono protetti da questo Firewall.
- Funzionamento router

  Utilizzando SCALANCE S come router, si disaccoppia la rete interna dalla rete esterna. La rete interna collegata da SCALANCE S diventa quindi una sotto-rete propria; SCALANCE S deve essere indirizzato esplicitamente come router tramite il proprio indirizzo IP.
- Protezione per apparecchi e segmenti di rete

  La funzione di protezione Firewall può estendersi dal funzionamento di singoli apparecchi, più apparecchi, fino a interi segmenti di rete.
- Senza retroeffetti in caso di montaggio in reti piatte (modalità bridge)

  In caso di montaggio di uno SCALANCE S602 in un'infrastruttura di rete esistente non è necessario reimpostare gli apparecchi terminali.
- Unità Security e nodo interno come una unità (funzionamento Ghost)

  L'unità Security viene visto dall'esterno con l'indirizzo IP del nodo interno e l'indirizzo MAC dell'unità Security.
- NTP (protetto) S≥V4.0

  Per la sincronizzazione e la trasmissione sicura dell'ora.

Nodi di rete interni ed esterni

SCALANCE S602 ripartisce le reti in due aree:

- rete interna: aree protette con "nodi interni"

  I nodi interni sono quelli protetti da uno SCALANCE S.

- rete esterna: aree non protette con "nodi esterni"

  I nodi esterni sono quelli che si trovano fuori dall'area protetta.

Nota

Le reti interne vengono considerate sicure (fidate).

Collegare un segmento di rete interno a segmenti di rete esterni solo tramite SCALANCE S.

Non devono esistere altri percorsi di collegamento tra rete interna ed esterna!

1.6 Impiego di SCALANCE S612, S623 e S627-2M

Protezione totale - compito di SCALANCE S612, SCALANCE S623 e SCALANCE S627-2M

Grazie alla combinazione di diverse misure di sicurezza, quali firewall, router NAT/NAPT e VPN (Virtual Private Network) tramite IPsec Tunnel, le unità SCALANCE S612, SCALANCE S623 e SCALANCE S627-2M proteggono singoli dispositivi o intere celle di automazione da:

- spionaggio dei dati
- manipolazione dei dati
- accessi indesiderati

SCALANCE S consente questa protezione flessibile, senza retroeffetti, indipendente dal protocollo (dal layer 2 secondo IEEE 802.3) e senza utilizzo complicato.

SCALANCE S e SOFTNET Security Client vengono configurati con lo strumento di progettazione Security Configuration Tool.

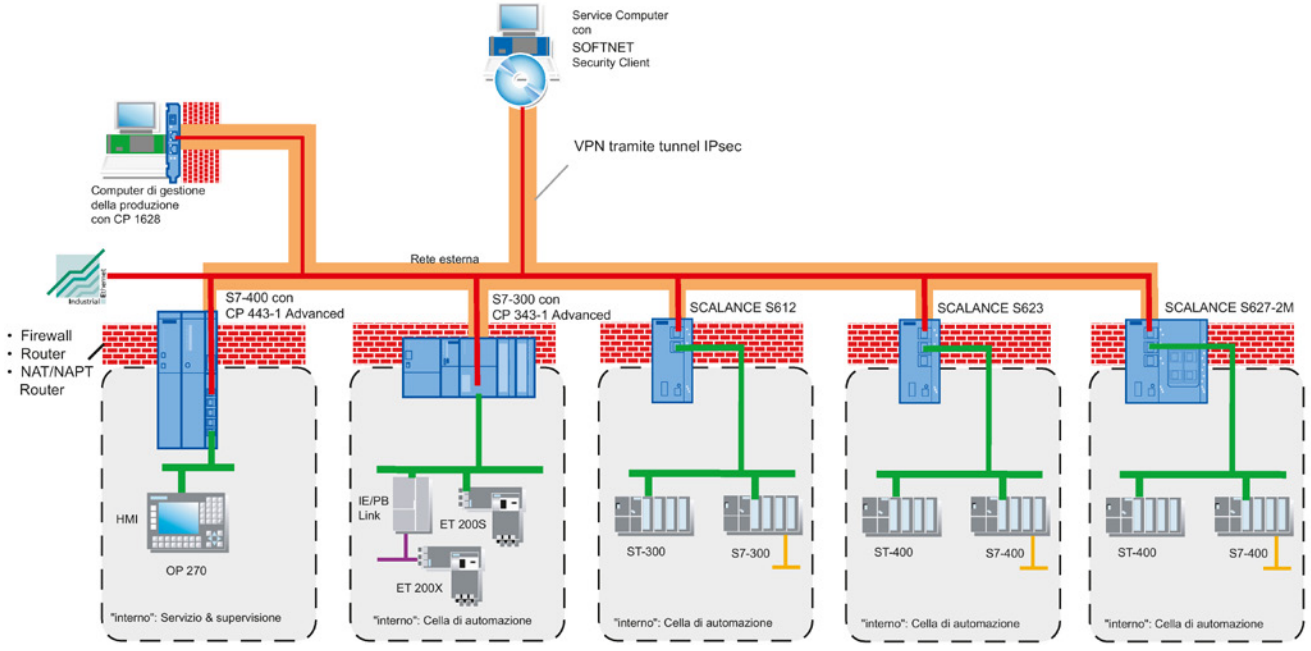


Figura 1-2 Configurazione di rete con SCALANCE S612, SCALANCE S623 e SCALANCE S627-2M

Funzioni di sicurezza

- Firewall
  - IP Firewall con Stateful Packet Inspection (layer 3 e 4)
  - Firewall anche per telegrammi Ethernet-"Non-IP" secondo IEEE 802.3

    (telegrammi layer 2; non è disponibile se viene utilizzato il funzionamento router)
  - Limitazione della larghezza di banda
  - Set di regole firewall globali
  - Set di regole IP specifiche per l'utente

  Tutti i nodi di rete che si trovano in un segmento di rete interno di uno SCALANCE S sono protetti da questo Firewall.
- Comunicazione protetta con IPsec Tunnel

  SCALANCE S può essere unito in un gruppo con altre unità Security tramite progettazione. Tra tutte le unità Security di un gruppo VPN vengono realizzati IPsec Tunnel (VPN, Virtual Private Network). Tutti i nodi interni di queste unità Security possono comunicare tra loro in modo sicuro tramite questo tunnel.
- Indipendenza dal protocollo

  La realizzazione dei tunnel comprende anche telegrammi Ethernet secondo IEEE 802.3 (telegrammi layer 2; non valido se viene utilizzata la modalità router).

  Attraverso il tunnel IPsec vengono trasmessi sia telegrammi IP, sia telegrammi Non-IP.
- PPPoE

  Point to Point Protocol over Ethernet (RFC 2516) per il rilevamento automatico di indirizzi IP dal provider in modo che non sia necessario l'impiego di un router DSL separato.
- Client per DNS dinamico (client DDNS)

  Domain Name Service dinamico per l'impiego di indirizzi IP dinamici se in ambiti di manutenzione remota uno SCALANCE S viene utilizzato in combinazione con il SOFTNET Security Client, unità SCALANCE M, unità SCALANCE S o altri clienti VPN come server VPN.
- SNMPv3

  Per la trasmissione continua sicura delle informazioni di analisi della rete.
- Router operation

  Utilizzando SCALANCE S come router, si collega la rete interna alla rete esterna. La rete interna collegata tramite SCALANCE S diventa quindi una sotto-rete propria.
- Protezione per apparecchi e segmenti di rete

  La funzione di protezione Firewall e VPN può estendersi dal funzionamento di singoli apparecchi, più apparecchi, fino a interi segmenti di rete.
- Interfaccia DMZ supplementare S62x

  In una zona demilitarizzata (DMZ) è possibile posizionare server per i quali può essere controllato e limitato l'accesso ad altre reti (rete esterna non sicura, rete interna sicura). In

questo modo possono essere messe a disposizione entrambe le reti sicure in base ai servizi e ai dati, senza consentire una comunicazione diretta tra loro per entrambe le reti.

- Senza retroeffetti in caso di montaggio in reti piatte (modalità bridge)

  I nodi di rete interni possono essere trovati senza progettazione. In caso di montaggio di uno SCALANCE S in un'infrastruttura di rete esistente non è quindi necessario riconfigurare gli apparecchi terminali.

  L'unità Security cerca di trovare nodi interni; i nodi interni che non possono essere trovati in questo modo devono perciò essere progettati.

- Autenticazione utente mediante server RADIUS S≥V4.0

  Su un server RADIUS possono essere memorizzati centralmente nomi utente, password e ruoli di utenti. L'autenticazione di questi utenti avviene quindi mediante il server RADIUS.

- NTP (protetto) S≥V4.0

  Per la sincronizzazione e la trasmissione sicura dell'ora.

Nodi di rete interni, nodi di rete esterni, nodi di rete DMZ

SCALANCE S ripartisce le reti in diverse aree:

- Rete interna: aree protette con "nodi interni"

  I nodi interni sono tutti i nodi protetti da uno SCALANCE S.

- Rete esterna: aree non protette con "nodi esterni"

  I nodi esterni sono quelli che si trovano fuori dall'area protetta.

- Rete DMZ: aree protette con i "Nodi DMZ" S62x

  I nodi DMZ sono sono tutti i nodi che si trovano nella DMZ e che sono protetti da uno SCALANCE S.

Nota

Le reti collegate all'interfaccia interna vengono considerate sicure (accreditate).

Collegare un segmento di rete interno a segmenti di rete esterni di un altro livello di sicurezza (rete esterna, rete DMZ) solo tramite SCALANCE S.

Non devono esistere altri percorsi di collegamento tra rete interna e una rete con altri livelli di sicurezza.

1.7 Impiego dell'interfaccia DMZ di SCALANCE S623 e SCALANCE S627-2M

Settori di impiego dell'interfaccia DMZ

Oltre alle funzioni di SCALANCE S612, SCALANCE S623 e SCALANCE S627-2M è equipaggiato con una terza interfaccia (DMZ) alla quale può essere collegata un'ulteriore rete.
L'interfaccia può svolgere diverse funzioni (non simultaneamente) in funzione del settore d'impiego:

- Configurazione di una DMZ
- Punto terminale per il collegamento via tunnel VPN
- Interfaccia di sincronizzazione per ridondanza router e firewall
- ...

Configurazione di una DMZ

Con SCALANCE S623 und dem SCALANCE S627-2M è possibile configurare una DMZ (zona demilitarizzata) sull'interfaccia supplementare. Una DMZ viene spesso utilizzata se devono essere forniti servizi per una rete non protetta e la rete sicura, che fornisce dati per questi servizi, deve essere disaccoppiata dalla rete non protetta.

Nella DMZ possono essere ad es. essere presenti Terminal Server con software di manutenzione e di diagnostica installati che possono essere utilizzati dalla rete esterna da utenti autorizzati.

In casi applicativi DMZ caratteristici l'utente deve progettare regole firewall in modo che da Internet siano possibili accessi (esterni) ai server nella DMZ (event. protetti ulteriormente con un tunnel VPN), ma non ad apparecchi nell'area protetta (interna).

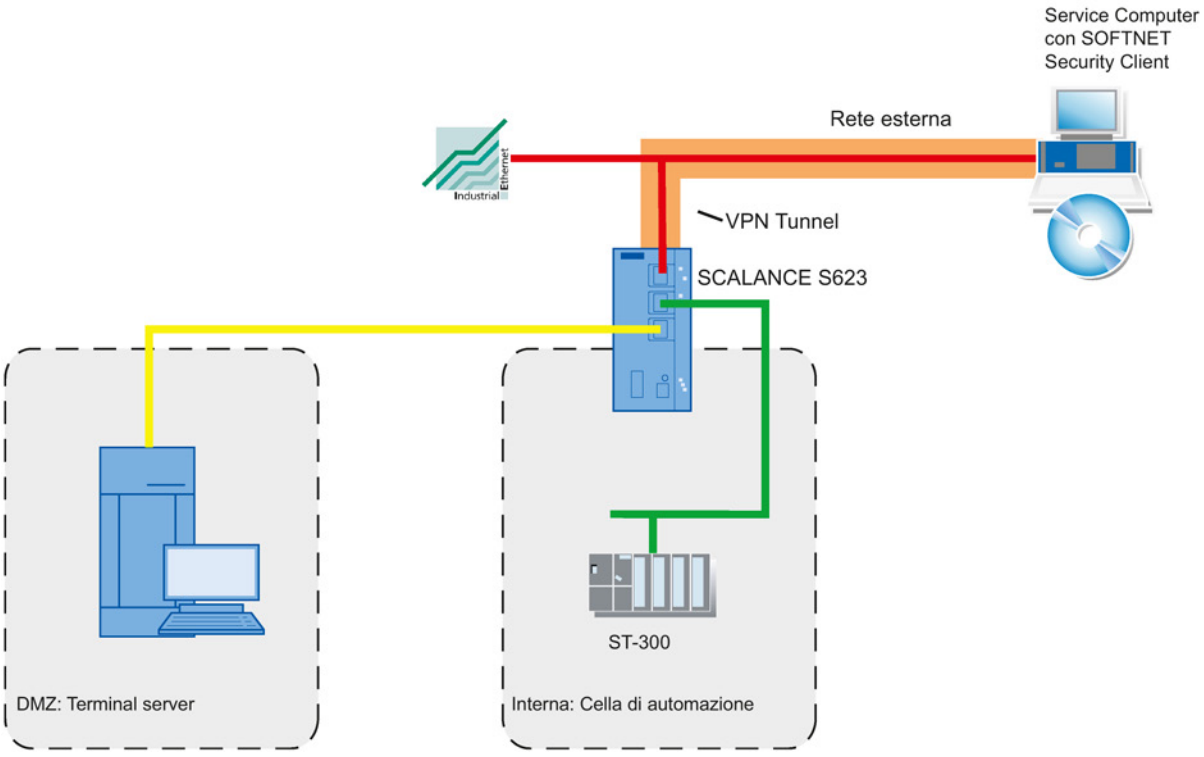


Figura 1-3 Configurazione di una DMZ

Una configurazione generica, nella quale l'interfaccia DMZ viene utilizzata per la configurazione di una DMZ, viene eseguita e documentata nel capitolo "4.2 SCALANCE S come firewall tra rete esterna e DMZ" del manuale "SIMATIC NET Industrial Ethernet Security - Configurazione di Security".

Punto terminale per il collegamento via tunnel VPN

L'interfaccia DMZ può essere utilizzata come punto terminale di un tunnel VPN. In questo contesto l'interfaccia DMZ è collegata a Internet tramite un modem DSL collegato e viene utilizzata tramite PPPoE. Il tunnel VPN consente la comunicazione sicura con ad es. un'unità di automazione collegata all'interfaccia interna di un'ulteriore unità Security.

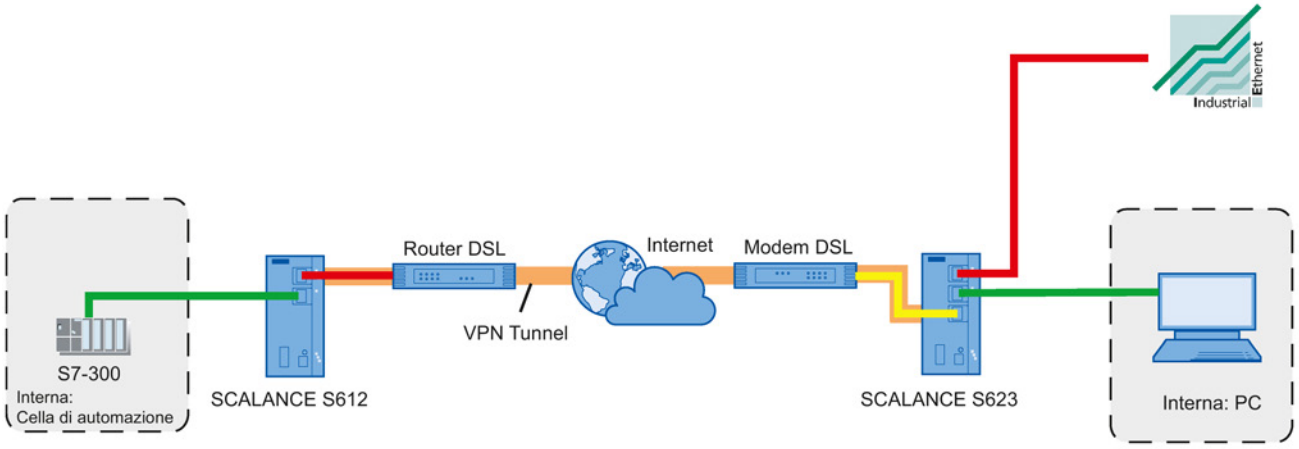


Figura 1-4 Punto terminale per il collegamento via tunnel VPN

Una configurazione generica, nella quale l'interfaccia DMZ viene utilizzata come punto terminale di un tunnel VPN, viene eseguita nel capitolo "5.2 Tunnel VPN tra SCALANCE S623 e SCALANCE S612" del manuale "SIMATIC NET Industrial Ethernet Security - Configurazione di Security".

Interfaccia di sincronizzazione per ridondanza router e firewall S62x ≥ V4.0

Con l'impiego di due unità Security del tipo SCALANCE S623 o SCALANCE S627-2M il guasto di un'unità Security può essere compensato con la ridondanza router e firewall. In questo caso le due unità Security vengono utilizzate in modalità routing e collegate rispettivamente ad una rete esterna ed interna nella quale è già attiva un'unità Security. Se l'unità Security attiva si guasta, l'unità Security passiva assume la sua funzione come router o firewall. Per garantire un comportamento funzionalmente identico di entrambe le unità Security, queste ultime vengono collegate tra loro tramite le relative interfacce DMZ e la relativa configurazione viene sincronizzata durante il funzionamento.

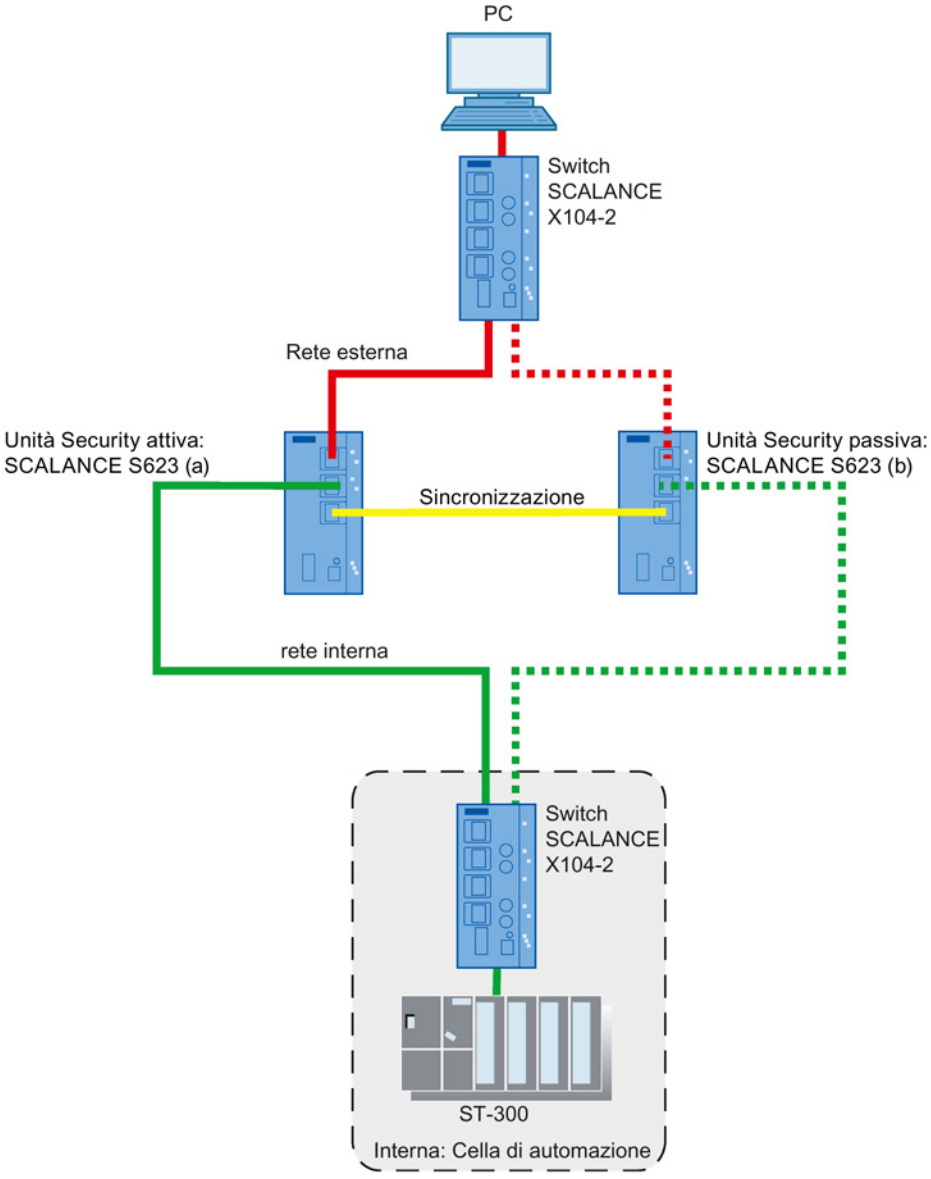


Figura 1-5 Ridondanza router e firewall

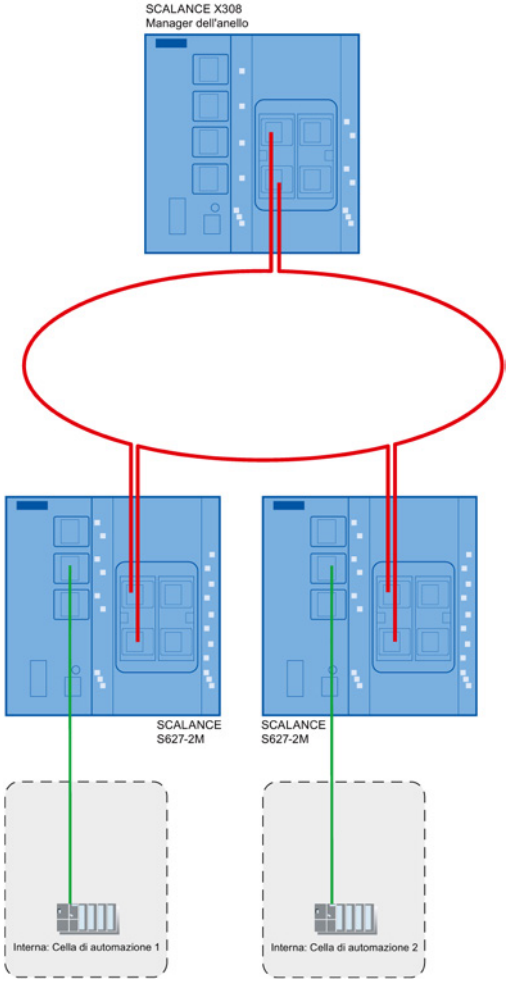
1.8 Impiego delle porte dei modulo mediali di SCALANCE S627-2M

Integrazione nelle topologie ad anello

Oltre alle funzioni di SCALANCE S623, SCALANCE S627-2M dispone di due slot modulo mediale nei quali può essere inserito rispettivamente un modulo mediale elettrico o ottico con due porte. In questo modo l'interfaccia esterna ed interna può essere ampliata rispettivamente di due porte. In modalità routing le porte supplementari dell'unità Security possono essere utilizzate per il collegamento dell'interfaccia esterna e interna alle topologie ad anello.

Ridondanza dell'anello con MRP o HRP

SCALANCE S627-2M supporta i protocolli MRP e HRP sulle porte modulo mediale dell'interfaccia esterna ed interna come client. Come nodo di un anello MRP/HRP uno SCALANCE S627-2M può proteggere una cella di automazione sottostante o un anello sottostante. Questa protezione può essere eseguita anche in modo ridondante. I guasti di linea vengono riconosciuti da un manager dell'anello separato, ad es. da uno SCALANCE X308, e compensati dalla deviazione del percorso di comunicazione.



1.9 Impiego di CP 343-1 Advanced e CP 443-1 Advanced

Concetto di protezione della cella - compito del CP x43-1 Adv.

Con Industrial Ethernet Security è possibile proteggere singoli apparecchi, celle di automazione o segmenti di rete di una rete Ethernet. Inoltre la trasmissione dei dati può essere protetta dalla combinazione di diverse misure di sicurezza quali firewall, NAT/NAPT Router e VPN (Virtual Private Network) tramite IPsec Tunnel da:

- spionaggio dei dati
- manipolazione dei dati
- accessi indesiderati

Le funzioni Security del CP x43-1 Adv. vengono configurare con lo strumento di progettazione Security Configuration Tool, integrato in STEP 7.

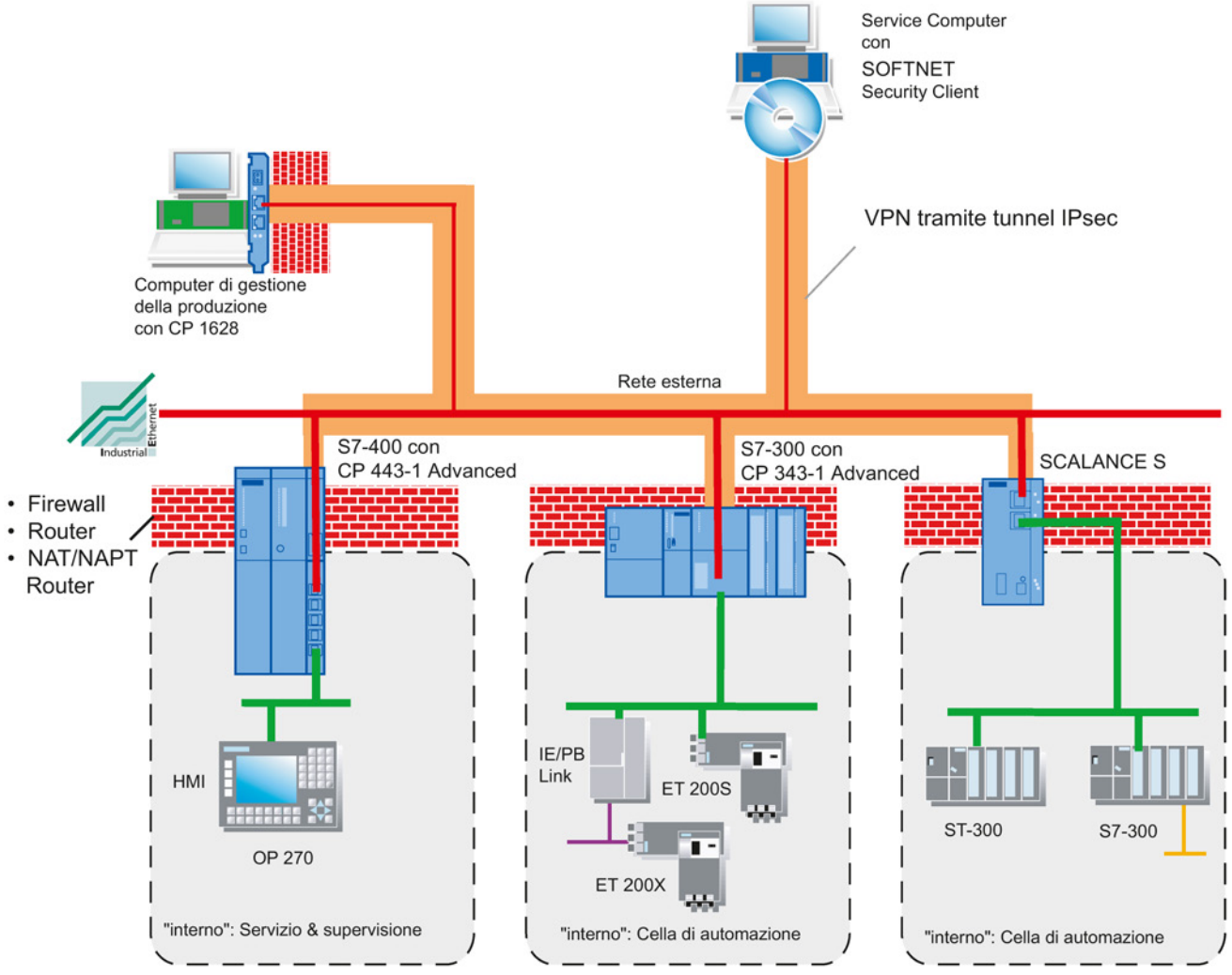


Figura 1-6 Configurazione della rete con CP x43-1 Adv.

Funzioni di sicurezza

- Firewall
  - IP Firewall con Stateful Packet Inspection (layer 3 e 4)
  - Firewall anche per telegrammi Ethernet-"Non-IP" secondo IEEE 802.3 (layer 2)
  - Limitazione della larghezza di banda
  - Set di regole firewall globali

  Tutti i nodi di rete che si trovano in un segmento di rete interno di un CP x43-1 Adv. sono protetti da questo Firewall.
- Comunicazione protetta con IPsec Tunnel

  Il CP x43-1 Adv. può essere unito in un gruppo con altre unità Security tramite progettazione. Tra tutte le unità Security di un gruppo VPN vengono realizzati IPsec Tunnel (VPN). Tutti i nodi interni di queste unità Security possono comunicare tra loro in modo sicuro tramite questo tunnel.
- Logging

  Per la trasmissione è possibile salvare gli eventi in file Log, che possono essere letti con lo strumento di progettazione o inviati automaticamente ad un Syslog Server.
- HTTPS

  Per la trasmissione codificata di pagine Web, ad es. durante il controllo del processo.
- FTPS

  Per la trasmissione codificata di file.
- NTP (protetto)

  Per la sincronizzazione e la trasmissione sicura dell'ora.
- SNMPv3

  Per la trasmissione continua sicura delle informazioni di analisi della rete.
- Protezione per apparecchi e segmenti di rete

  La funzione di protezione Firewall e VPN può estendersi dal funzionamento di singoli apparecchi, più apparecchi, fino a interi segmenti di rete.

Nodi di rete interni ed esterni:

Il CP x43-1 Adv. ripartisce le reti in due aree:

- rete interna: aree protette con "nodi interni"

  I nodi interni sono quelli protetti da un CP x43-1 Adv.

- rete esterna: aree non protette con "nodi esterni"

  I nodi esterni sono quelli che si trovano fuori dall'area protetta.

Nota

Le reti interne vengono considerate sicure (fidate).

Collegare un segmento di rete interno a segmenti di rete esterni solo tramite il CP x43-1 Adv.

Non devono esistere altri percorsi di collegamento tra rete interna ed esterna.

Informazioni relative alle funzioni generali del CP x43-1 Adv.

Nel presente manuale si trovano informazioni relative alle funzioni Security del CP x43-1 Adv. Per le descrizioni relative alle funzioni generali vedere:

- /1/ (Pagina 268)
- /2/ (Pagina 268)

1.10 Impiego del CP 1628

Concetto di protezione della cella - compito del CP 1628

I meccanismi di sicurezza integrati del CP 1628 consentono la protezione di sistemi di computer compresa la relativa comunicazione dei dati all'interno di una rete di automazione o l'accesso remoto protetto tramite Internet. Il CP 1628 consente l'accesso a singoli apparecchi o a intere celle di automazione protette tramite unità Security e consente collegamenti protetti su strutture di rete non protette.

Grazie alla combinazione di diverse misure di sicurezza quali il firewall o la VPN (Virtual Private Network) tramite il tunnel IPsec il CP 1628 protegge da:

- spionaggio dei dati
- manipolazione dei dati
- accessi indesiderati

Le funzioni Security del CP 1628 vengono configurare con lo strumento di progettazione Security Configuration Tool, integrato in STEP 7.

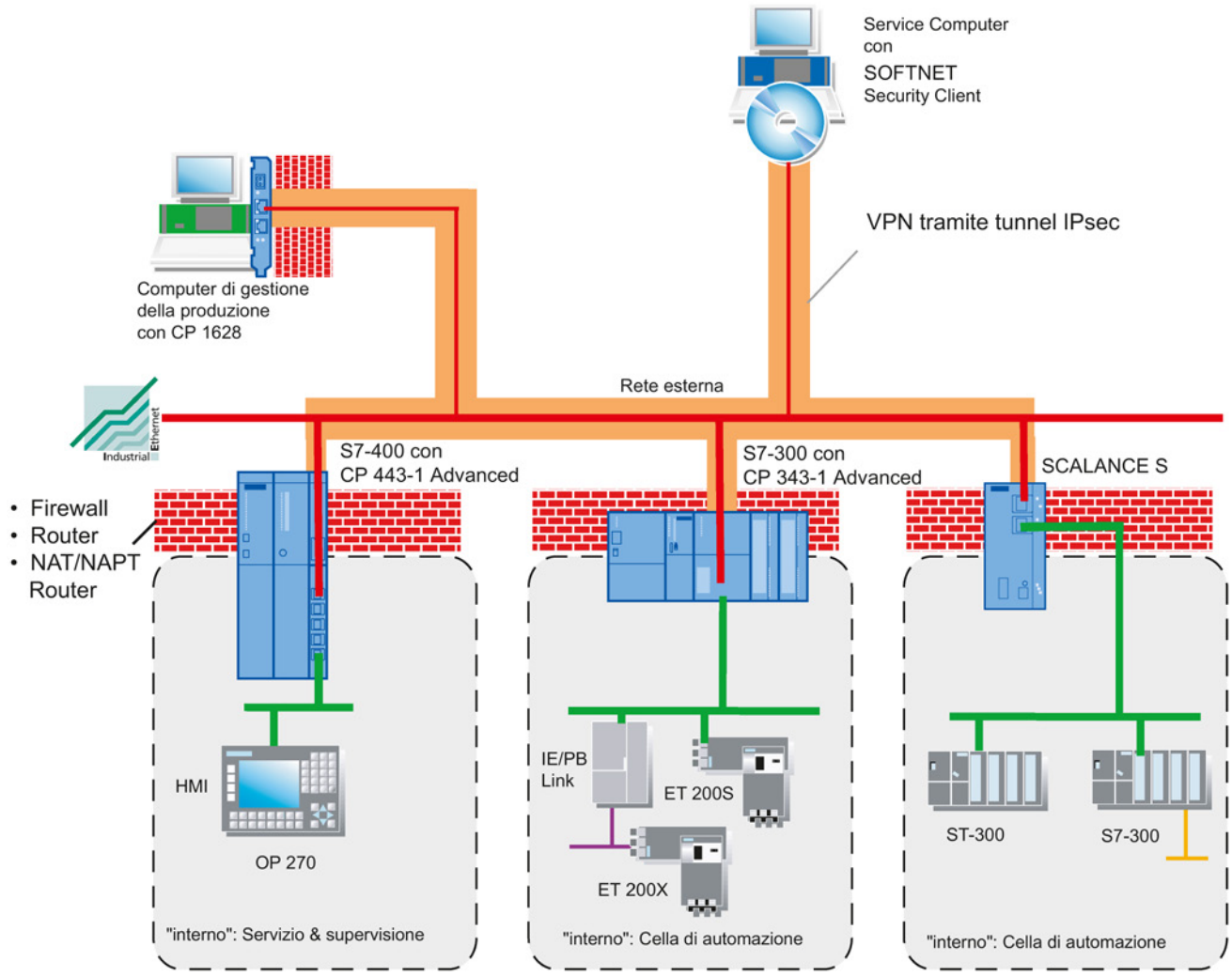


Figura 1-7 Configurazione della rete con il CP 1628

Funzioni di sicurezza

- Firewall
  - IP Firewall con Stateful Packet Inspection (layer 3 e 4)
  - Firewall anche per telegrammi Ethernet-"Non-IP" secondo IEEE 802.3 (layer 2)
  - Limitazione della larghezza di banda
  - Regole firewall globali
- Comunicazione protetta con IPsec Tunnel

  Il CP 1628 può essere unito in un gruppo con altre unità Security tramite progettazione. Tra tutte le unità Security di un gruppo VPN vengono realizzati IPsec Tunnel (VPN, Virtual Private Network).

- Logging

  Per la trasmissione è possibile salvare gli eventi in file Log, che possono essere letti con lo strumento di progettazione o inviati automaticamente ad un Syslog Server.

- NTP (protetto)

  Per la sincronizzazione e la trasmissione sicura dell'ora.

- SNMPv3

  Per la trasmissione continua sicura delle informazioni di analisi della rete.

Informazioni relative alle funzioni generali del CP 1628

Nel presente manuale si trovano informazioni relative alle funzioni Security del CP 1628. Per le descrizioni relative alle funzioni generali vedere

- /11/ (Pagina 271)

1.11 Progettazione e amministrazione

Riassunto dei punti più importanti

L'interazione con lo strumento di progettazione Security Configuration Tool consente un impiego semplice e sicuro delle unità Security:

- Progettazione senza nozioni esperti IT con il Security Configuration Tool

  Con il Security Configuration Tool anche non esperti IT possono progettare un'unità Security. In modalità estesa, in caso di necessità, è possibile eseguire impostazioni complicate.

- Comunicazione amministrativa protetta

  La trasmissione delle impostazioni è firmata e codificata e può essere eseguita solo da personale autorizzato.

- Protezione contro l'accesso nel Security Configuration Tool

  Grazie alla gestione utenti del Security Configuration Tool, è garantita una protezione da accesso per le unità Security e i dati di progettazione.

- Supporto dati C-PLUG impiegabile

  Il C-PLUG è un supporto dati innestabile, sul quale sono salvati i dati di configurazione codificati. In caso di sostituzione di un'unità Security esso consente la configurazione senza PG/PC, se l'unità Security supporta un mantenimento dei dati sul C-PLUG.

Progettazione con Security Configuration Tool 2

Il Security Configuration Tool è lo strumento di progettazione fornito con unità Security.

Il presente capitolo semplifica l'approccio con la superficie operativa e il tipo di funzionamento dello strumenti di progettazione.

Qui viene descritto come configurare, comandare e gestire i progetti Security.

Altre informazioni

Nei seguenti capitoli di questo manuale viene descritto in modo dettagliato come si configurano le unità Security e il tunnel IPsec.

Le informazioni dettagliate sulle finestre di dialogo e i parametri impostabili si trovano anche nella guida in linea. Alla guida è possibile accedere con il tasto F1 o con il pulsante "Help" nella relativa finestra di dialogo.

2.1 Panoramica - Potenzialità e tipi di funzionamento

Potenzialità

Lo strumento di progettazione Security Configuration Tool si utilizza per i seguenti compiti:

- Progettazione delle unità Security
- Progettazione di SOFTNET Security Client
- Creazione dei dati di configurazione VPN per SCALANCE M
- Creazione di file di configurazione VPN per dispositivi VPN di altri produttori
- Funzioni di test e di diagnostica, indicazioni di stato

Due modalità di funzionamento del Security Configuration Tool

Il Security Configuration Tool può essere richiamato nelle seguenti modalità di funzionamento:

- Security Configuration Tool Standalone:
  - Può essere richiamato indipendentemente da STEP 7
  - Nessuna progettazione Security possibile di CP
- Security Configuration Tool integrato in STEP 7:
  - Può essere richiamato solo da STEP 7.
  - Nel progetto deve trovarsi almeno un CP con funzione Security attivata
  - La funzionalità di Security Configuration Tool Standalone viene estesa della possibilità di progettare funzioni Security per CP

Visualizzazione di progettazione offline e visualizzazione di diagnostica online

Il Security Configuration Tool dispone di una visualizzazione di progettazione offline e di una visualizzazione di diagnostica online:

- Visualizzazione di progettazione offline

  Nel modo di funzionamento offline la progettazione dei dati di configurazione viene eseguita per l'unità corrispondente. Prima dell'operazione di caricamento non deve esistere un collegamento con questa unità.

- Online

  La modalità online serve al test e alla diagnostica di un'unità Security.

Due modalità di comando

Nella visualizzazione di progettazione offline il Security Configuration Tool mette a disposizione due modalità di comando:

- Modalità standard

  Lo Standard Mode è preimpostato nel Security Configuration Tool. Questa modalità consente una rapida e semplice progettazione per il funzionamento delle unità Security.

- Modalità estesa

  Nella modalità estesa esistono possibilità di impostazione estese che consentono inoltre l'impostazione individuale delle regole del firmware, delle impostazioni Log, delle regole NAT/NAPT, dei nodi VPN e di funzionalità di sicurezza estese.

Tipo di funzionamento - Sicurezza e coerenza

- Accesso solo per utenti autorizzati

  Ciascun progetto può essere protetto contro l'accesso non autorizzato mediante inserimento del nome utente e della password. Con le direttive password è possibile stabilire predefinizioni specifiche per il progetto per l'inserimento della password.

- Dati di progetto coerenti

  Già durante l'inserimento nelle singole finestra di dialogo vengono eseguiti controlli di coerenza. Inoltre è possibile effettuare in qualsiasi momento un controllo di coerenza esteso nel progetto in tutte le finestre di dialogo.

  Nelle unità Security possono essere caricati solo dati di progetto coerenti.

- Protezione dei dati del progetto tramite codifica

  I dati del progetto e di configurazione sono protetti da codifica sia nel file del progetto, se esistente, sia nel C-PLUG (non per CP 1628).

2.2 Installazione del Security Configuration Tool

2.2.1 Sistemi operativi supportati

Sistemi operativi supportati

Vengono supportati i seguenti sistemi operativi:

- Microsoft Windows XP a 32 bit + Service Pack 3
- Microsoft Windows 7 Professional a 32/64 bit
- Microsoft Windows 7 Professional a 32/64 bit + Service Pack 1
- Microsoft Windows 7 Ultimate a 32/64 bit
- Microsoft Windows 7 Ultimate a 32/64 bit + Service Pack 1
- Windows Server 2008 R2 a 64 bit
- Windows Server 2008 R2 a 64 bit + Service Pack 1

Nota

Prima dell'installazione del Security Configuration Tool leggere assolutamente il file "LEGGIMI.htm" presente nel DVD. In questo file sono eventualmente indicate avvertenze importati e le ultime modifiche.

SCALANCE S - Procedimento

Lo strumento di progettazione Security Configuration Tool si installa dal DVD del prodotto fornito.

- Inserire il DVD del prodotto nel drive DVD-ROM. Con la funzione Autorun attivata l'interfaccia utente dalla quale è possibile eseguire l'installazione viene avviata automaticamente.

o

- Avviare l'applicazione "start.exe" presente sul DVD del prodotto fornito.

CP x43-1 Adv. - Procedimento

Lo strumento di progettazione Security Configuration Tool si installa dal supporto dati STEP 7. Il file di installazione si trova nel supporto dati STEP 7, nella cartella per i componenti software opzionali.

CP 1628 - Procedimento

Lo strumento di progettazione Security Configuration Tool si installa dal supporto dati fornito che contiene i dati driver del CP 1628.

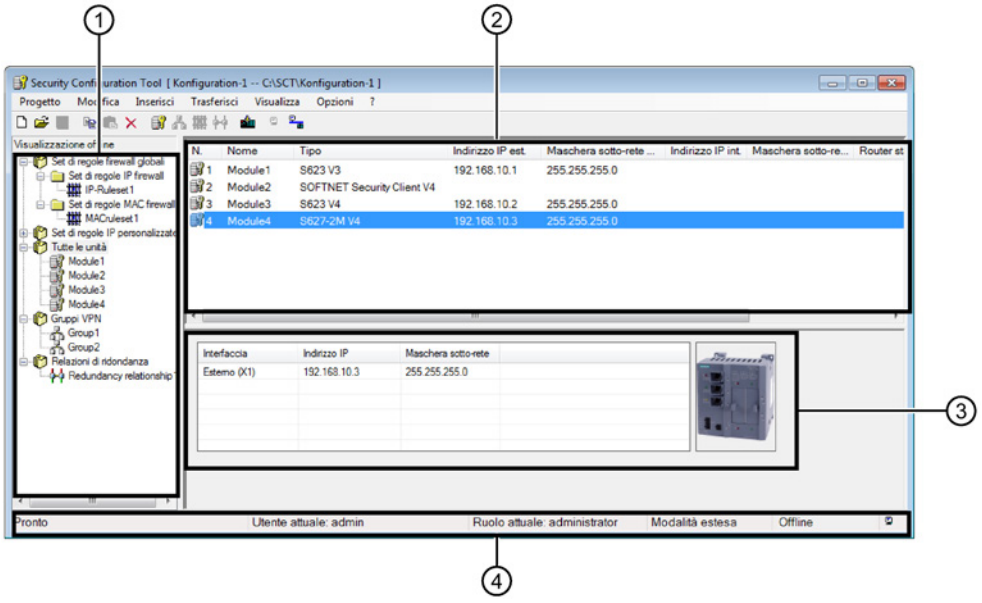
- Inserire il supporto dati nel drive DVD-ROM. Con la funzione Autorun attivata l'interfaccia utente dalla quale è possibile eseguire l'installazione viene avviata automaticamente.

o

- Avviare l'applicazione "setup.exe" presente sul supporto dati fornito.

2.3 Superficie operativa e voci di menu

Struttura dell'interfaccia di comando in modalità estesa



① Area di navigazione:

- Set di regole firewall globali

  L'oggetto contiene i set di regole globali firewall progettati Altre cartelle distinguono tra:
  - Firewall set di regole IP
  - Firewall set di regole MAC
- Set di regole IP specifiche per l'utente S≥V3.0
- Tutte le unità

  L'oggetto contiene tutte le unità progettate e le configurazioni SOFTNET del progetto.
- Gruppi VPN

  L'oggetto contiene tutti i gruppi VPN generati.
- Relazioni di ridondanza S≥V4.0

  L'oggetto contiene tutte le relazioni di ridondanza generate del progetto.

② Area del contenuto:

Selezionando un oggetto nell'area di navigazione, nell'area del contenuto si ottengono informazioni dettagliate su questo oggetto.

Per alcune unità Security in questa area è possibile osservare e adattare gli estratti delle configurazioni dell'interfaccia.

Facendo doppio clic sulle unità Security, se esse offrono le possibilità di configurazione corrispondenti, vengono aperte le finestre di dialogo delle proprietà per l'inserimento di ulteriori parametri.

③ Finestra dei dettagli:
La finestra dei dettagli contiene informazioni supplementari relative all'oggetto selezionato e consente ad un gruppo VPN nel rispettivo contesto la progettazione di proprietà VPN specifiche per il collegamento.
La finestra dei dettagli può essere disattivata e attivata mediante il menu "Visualizza".

④ Riga di stato:
La riga di stato illustra gli stati di comando e i messaggi di stato attuali. Ne fanno parte:

- L'utente attuale e il tipo di utente
- La visualizzazione di comando - modalità standard / modalità estesa
- Lo stato operativo - Online / Offline

Barra dei simboli

Qui di seguito è riportata una panoramica dei simboli selezionabili nella barra dei simboli e del relativo significato.

Icona	Significato / Osservazioni
	Crea un nuovo progetto.
	Apre un progetto esistente.
	Salva il progetto aperto nel percorso attuale con il nome del progetto.
	Copia l'oggetto selezionato.
	Inserisci l'oggetto dagli appunti.
	Cancella l'oggetto selezionato.
	Crea una nuova unità. Il simbolo è attivo solo all'interno dell'area di navigazione se ci si trova nella cartella "Tutte le unità".
	Crea un nuovo gruppo VPN. Il simbolo è attivo solo all'interno dell'area di navigazione ci si trova nella cartella "Gruppi VPN".
	Creazione di un nuovo set di regole IP globale / set di regole MAC o di un set di regole IP personalizzato. Il simbolo è attivo solo se all'interno di un'area di navigazione ci si trova in una sotto-cartella di "Set di regole firewall globali" o su una cartella "Set di regole IP personalizzate"
	Creazione di una nuova relazione di ridondanza. Il simbolo è attivo solo all'interno dell'area di navigazione se ci si trova nella cartella "Relazioni di ridondanza".

Icona	Significato / Osservazioni
	 Caricamento della configurazione nelle unità Security selezionate o impostazione dei dati di configurazione per SOFTNET Security Client / SCALANCE M.
	Commutazione nella modalità offline.
	Commutazione nella modalità online.

Barra dei menu

Qui di seguito è riportata una panoramica delle voci di menu selezionabili e del loro significato.

Voce di menu		Significato / Osservazioni	Combinazione dei tasti
Project ▸…		Funzioni per le impostazioni specifiche del progetto, nonché caricamento e salvataggio dei file del progetto.	
CP	Nuovo...	Crea un nuovo progetto. Per CP: I progetti vengono creati con la progettazione STEP 7.	
CP	Apri...	Apre un progetto esistente. Per CP: I progetti esistenti possono essere aperti solo tramite i progetti STEP 7.	
	Salva	Salva il progetto aperto nel percorso attuale con il nome del progetto.	Ctrl + S
CP	Salva con nome...	Salva il progetto aperto nel percorso selezionabile con il nome del progetto. Per CP: Il progetto è parte del progetto STEP 7. Il percorso non può essere modificato.	
	Proprietà...	Si apre la finestra di dialogo delle proprietà del progetto.	
CP	Progetti aperti per ultimi	Possibilità di selezione diretta dei progetti elaborati finora. Per CP: I progetti esistenti possono essere aperti solo tramite STEP 7.	
	Exit	Chiudi progetto.	
Edit ▸…		Voci di menu solo in modalità offline **Avvertenza** Nel progetto attivato le funzioni possono essere selezionate in parte anche tramite il menu contestuale.	
CP	Copy	Copia l'oggetto selezionato.	Ctrl + C
	Paste	Riprende e inserisce l'oggetto dalla memoria intermedia.	Ctrl + V
	Del	Cancella l'oggetto selezionato.	Canc
	Rename	Rinomina l'oggetto selezionato.	F2
	Nuovo certificato...	Creazione di un nuovo certificato del gruppo per l'unità selezionata nell'area del contenuto dopo la selezione del rispettivo gruppo VPN.	
	Sostituisci unità ...	Sostituzione dell'unità Security selezionata con un'altra.	
	Proprietà ...	Apre la finestra di dialogo delle proprietà dell'oggetto selezionato.	F4
	Diagnostica online ...	Accede alle funzioni di test e di diagnostica.	

Voce di menu		Significato / Osservazioni	Combinazione dei tasti
Insert ▸…		Voci di menu solo in modalità offline	
	Unità	Creazione di una nuova unità Security. La voce di menu è attiva solo se nell'area di navigazione è selezionata un'unità Security o un gruppo VPN.	Ctrl + M
	Group	Crea un nuovo gruppo VPN. La voce di menu è attiva solo se nell'area di navigazione è selezionato un oggetto gruppi.	Ctrl + G
	Set di regole firewall	Creazione di un nuovo set di regole IP firewall globale, di un set di regole MAC o di un set di regole IP personalizzato. La voce di menu è attiva solo se nell'area di navigazione è selezionato un oggetto firewall. La voce di menu è visibile solo in modalità estesa.	Ctrl + F
	Relazione di ridondanza	Creazione di una nuova relazione di ridondanza. La voce di menu è attiva solo all'interno dell'area di navigazione se ci si trova nella cartella "Relazioni di ridondanza".	Ctrl + R
Transfer ▸…			
	All'unità/alle unità...	Caricamento della configurazione nell'unità/nelle unità Security selezionate o creazione dei dati di configurazione per SOFTNET Security Client / SCALANCE M / dispositivi VPN / NCP VPN Client (Android). Osservazione: possono essere caricati solo dati di progetto coerenti. Per CP: I dati del progetto possono essere caricati solo tramite STEP 7.	
	A tutte le unità...	Caricamento della configurazione in tutte le unità Security. Osservazione: possono essere caricati solo dati di progetto coerenti.	
	Stato della configurazione…	Visualizza in un elenco lo stato di configurazione delle unità Security progettate.	
	Trasferimento del firmware ...	Caricamento del nuovo firmware nell'unità Security selezionata. Per CP S7: Il firmware viene caricato nel CP tramite il centro di aggiornamento della diagnostica Web.	
View ▸…			
	Modalità estesa	Commuta dalla modalità standard (preimpostazione) alla modalità estesa. **Attenzione** Una commutazione nella modalità estesa per il progetto attuale non può più essere annullata.	Ctrl + E
	Mostra finestra dei dettagli	Mostra e nasconde i dettagli supplementari relativi all'oggetto selezionato.	Ctrl + Alt + D

Voce di menu		Significato / Osservazioni	Combinazione dei tasti
	Offline	Preimpostazione. Commutazione nella visualizzazione di progettazione offline.	Ctrl + Maiu + D
	Online	Commutazione nella visualizzazione di diagnostica online.	Ctrl + D
Options ▸…			
	Servizi IP...	Apre la finestra di dialogo per le definizioni dei servizi per le regole IP Firewall. La voce di menu è visibile solo in modalità estesa.	
	Servizi MAC...	Apre la finestra di dialogo per le definizioni dei servizi per le regole MAC Firewall. La voce di menu è visibile solo in modalità estesa.	
	Adattatore di rete...	Tramite l'adattatore di rete selezionato a SCALANCE S viene assegnato un indirizzo IP.	
	Lingua...	Seleziona la lingua visualizzata nell'interfaccia SCT. Per il SCT in STEP 7 la lingua dell'interfaccia SCT viene definita tramite la selezione della lingua in STEP 7.	
	File Log...	Visualizzazione dei file Log salvati.	
	Symbolic Names...	Impostazione di nomi simbolici per indirizzi IP o MAC.	
	Configurazione del server NTP...	Imposta e modifica il server NTP	
	Configurazione del server RADIUS...	Creazione e modifica del server RADIUS.	
	Controlli della coerenza...	Controllare la coerenza dell'intero progetto. Come risultato viene visualizzato un elenco dei risultati.	
	Gestione utenti...	Creazione e modifica di utenti e ruoli, assegnazione di diritti e definizione di direttive password.	
	Manager dei certificati...	Visualizza o importa / esporta certificati.	
Help ▸…			
	Argomenti della guida...	Guida alle funzioni e ai parametri che si trovano nell'SCT.	F1
	Informazioni...	Informazioni sulla versione dell'SCT.	

2.4 Creazione e gestione di progetti

2.4.1 Security Configuration Tool (variante standalone)

Progettazione con il Security Configuration Tool Standalone

Il Security Configuration Tool Standalone viene utilizzato per la creazione di progetti Security nei quali non vengono progettate unità Security che devono essere create e configurate in STEP 7.

Creare un nuovo progetto con la voce di menu "Progetto > Nuovo...". Esso comprende tutte le informazioni di configurazione e di gestione per uno o diversi SCALANCE S, SOFTNET Security Client, dispositivi SCALANCE M, dispositivi VPN e NCP VPN Client (Android). Creare un'unità nel progetto per ciascun dispositivo o per ciascuna configurazione.

2.4.2 Security Configuration Tool in STEP 7

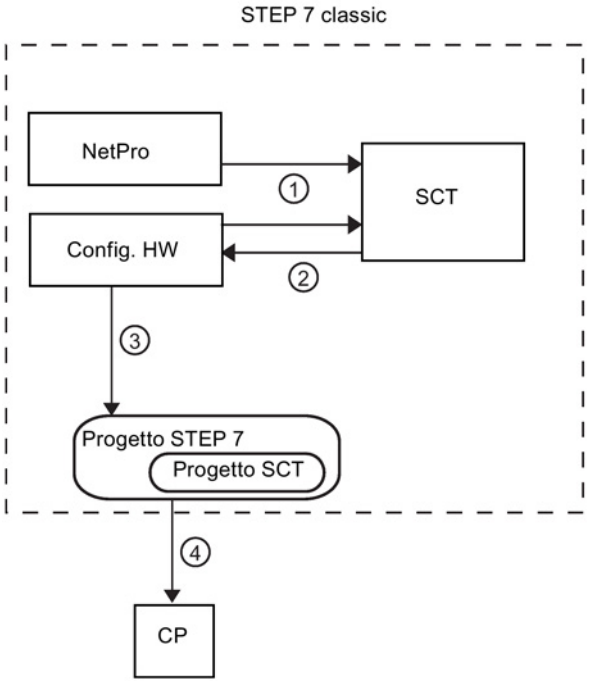
Progettazione

Il Security Configuration Tool in STEP 7 viene utilizzato per la creazione di progetti Security nei quali vengono progettate unità Security che devono essere create e configurate in STEP 7. Inoltre vengono supportati tutte le unità Security della variante Standalone.

Non appena in STEP 7 si attiva la funzione Security per un'unità Security, viene creato automaticamente un progetto SCT nel quale possono essere salvati e gestiti i dati della configurazione Security. Tutti i dati della configurazione Security vengono modificati internamente dall'SCT e il risultato viene ritrasmesso a STEP 7.

Interazione di STEP 7 e SCT

L'interazione di STEP 7 e SCT descritta in base alla seguente rappresentazione:



① Se con STEP 7 vengono eseguite impostazioni Security, SCT viene richiamato in quanto qui vengono modificati e gestiti i dati per Security.

Se in NetPro sono progettati collegamenti specificati, dopo il salvataggio e la compilazione per questi ultimi vengono create automaticamente regole firewall nell'SCT.

② Nell'SCT eseguire ulteriori impostazioni Security. l'SCT modifica internamente i dati e rinvia il risultato a STEP 7.

③ Le azioni quali "Salva con nome" e "Compila" avvengono all'interno di STEP 7. I dati Security vengono salvati come progetto SCT con un altro nome impostato automaticamente in una sotto-cartella del progetto STEP 7. Il nome e la posizione di memorizzazione non devono essere modificati. Per un progetto STEP 7 è possibile creare esattamente un progetto SCT. Un progetto SCT creato in STEP 7 con il Security Configuration Tool non può essere aperto con il Security Configuration Tool in modalità standalone.

④ I dati Security progettati del CP vengono caricati nell'unità tramite STEP 7.

Quali dati vengono migrati da STEP 7 a SCT e visualizzati nell'area del contenuto?

I seguenti dati di progettazione creati in STEP 7 vengono acquisiti automaticamente dall'SCT, ma non possono essere modificati:

- Nome apparecchio
- Indirizzo IP PROFINET IO
- Indirizzo IP GBit

- Maschera della sotto-rete PROFINET IO
- Maschera della sottorete GBit
- Indirizzo MAC dell'interfaccia GBit
- Router standard
- Indirizzo MAC PROFINET IO

Quali dati possono essere migrati nell'SCT e qui modificati?

Le seguenti funzioni utilizzate in STEP 7 possono essere migrate in SCT e qui modificate:

- Elenchi Access Control (Pagina 117)
- Utenti (Pagina 64)
- Server NTP (Pagina 185)

Le informazioni dettagliate su questo argomento si trovano nella guida in linea dell'SCT.

Alla guida è possibile accedere con il tasto F1 o con il pulsante "Help" nella relativa finestra di dialogo SCT.

Regole firewall automatiche per collegamenti progettati

Per i collegamenti specificati in STEP 7, in SCT vengono create automaticamente regole che abilitano la realizzazione del collegamento. Informazioni più dettagliate su questo argomento si trovano nel seguente capitolo:

- Regole firewall automaticamente riferite al collegamento (Pagina 141).

Per i collegamenti non specificati in SCT devono essere configurate regole firewall che abilitano la realizzazione del collegamento. Informazioni più dettagliate su questo argomento si trovano nel seguente capitolo:

- Firewall in modalità estesa (Pagina 134).

Esecuzione di impostazioni Security in STEP 7

Le impostazioni Security possono essere eseguite nel modo seguente:

- Tramite le singole schede nella proprietà dell'oggetto

  Nelle singole schede possono essere attivate ed eseguite funzioni Security specifiche per il CP. Durante l'esecuzione viene aperta la finestra di dialogo SCT corrispondente nella quale possono essere eseguite le impostazioni Security. Nelle seguenti schede possono essere eseguire le impostazioni Security:

	Scheda	Funzionamento	Descrizione
	Security	Attivare la Security	• Le funzioni Security nelle singole schede si attivano. • Si attiva il menu "Modifica" > "Security Configuration Tool" con il quale è possibile aprire il Security Configuration Tool. Qui possono essere eseguite altre impostazioni estese a tutte le unità Security, quali ad es. la creazione di gruppi VPN o l'aggiunta di unità Security non progettabili in STEP 7. • Se per l'unità Security sono stati progettati utenti in STEP 7, si apre la finestra "Migrazione dei dati del progetto rilevati per la sicurezza" con la quale è possibile migrare gli utenti STEP 7 nel Security Configuration Tool.
		Avvio della configurazione Security:	L'SCT si apre in una modalità panoramica nella quale è possibile configurare le proprietà specifiche per questa unità Security.
		Caricare successivamente online le regole firewall	Le impostazioni firewall adattate vengono generate e caricate nel CP senza causare un arresto del CP.
		Caricamento successivo online delle regole firewall (CP 1628)	Le impostazioni firewall adattate vengono generate e caricate nel CP.
	Utenti	Avvio della gestione utenti:	Avvia la gestione utenti SCT nella quale vengono creati utenti e ruoli e assegnati diritti.
	Protezione di accesso IP	Avvio della configurazione firewall	Durante l'attivazione di Security un elenco di accesso IP esistente viene migrato nel Security Configuration Tool mediante una conversione nelle regole firewall.
	FTP	Consenti accesso solo tramite FTPS	Avvia la gestione utenti SCT nella quale possono essere assegnati diritti FTP ad un ruolo.
		Avvio della gestione utenti:	
	Web	Consenti accesso solo tramite HTTPS	Avvia la gestione utenti SCT nella quale possono essere assegnati diritti Web ad un ruolo.
		Avvio della gestione utenti:	
	Sincronizzazione dell'ora	Configurazione NTP estesa	Avvia l'SCT in modalità di configurazione NTP.
	SNMP	Avvio della configurazione SNMP	Avvia l'SCT in modalità di configurazione SNMP. È possibile selezionare tra SNMPv1 o SNMPv3.
		Avvio della gestione utenti:	Avvia la gestione utenti SCT nella quale possono essere assegnati diritti SNMP ad un ruolo.

- Direttamente nell'SCT

  L'SCT si richiama in STEP 7 con il menu "Modifica" > "Security Configuration Tool". Oltre alle impostazioni nelle schede delle proprietà dell'oggetto qui si creano ad es. gruppi VPN o si aggiungono unità SCALANCE S. Le unità SCALANCE S possono essere progettate e caricate nell'SCT, ma i dati non vengono rinviati a STEP 7. Dopo aver chiuso l'SCT le unità non vengono visualizzate in STEP 7.

Nota

Indicazioni più dettagliate si trovano nella guida in linea di STEP 7 e nella guida in linea dell'SCT.

Informazioni generali relative a STEP 7 si trovano in /9/ (Pagina 270).

2.4.3 Migrazione di dati STEP 7

Migrazione di utenti dell'apparecchio STEP 7 nella gestione utenti SCT

Selezionare nella finestra di dialogo della migrazione il che modo gli utenti creati in STEP 7 devono essere migrati nella gestione utenti SCT. Qui sono disponibile le seguenti azioni per la selezione:

Azione	Descrizione
Acquisisci come...	L'utente viene migrato con un altro nome della gestione utenti SCT. Inserire il nome nella colonna "Nome utente migrato". Nell'SCT all'utente migrato viene assegnato un ruolo generato automatica-mente.
Unisci	Se in un progetto SCT è già creato un utente con lo stesso nome, entrambi gli utenti vengono uniti. Il ruolo dell'utente SCT viene esteso ai diritti selezionati dell'utente migrato.
Non acquisire	L'utente viene dell'unità Security non viene migrato nella gestione utenti SCT. Non è possibile una migrazione successiva.

Nota

I seguenti dati non vengono migrati

- Password di utenti già creati in STEP 7. Per questo motivo, per ogni utente selezionare in che modo esso deve essere migrato e indicare una nuova password con il pulsante "Assegna password".
- L'utente "everybody" definito dal sistema disponibile in STEP 7. Anche i relativi diritti per gli utenti migrati non vengono acquisiti.

Nota

Gli utenti e i relativi ruoli possono essere adattati dopo la migrazione nella gestione utente del Security Configuration Tool.

Migrazione di diritti dell'apparecchio STEP 7 nella gestione utenti SCT

Vengono migrati i seguenti diritti:

Diritto in STEP 7	Diritto dopo la migrazione nell'SCT	Servizio
Accesso ai simboli progettati	Applet: Lettura di variabili tramite i simboli progettati	SPS
	Applet: Scrittura di variabili tramite i simboli progettati	
Lettura di variabili tramite indirizzi assoluti	Applet: Lettura di variabili tramite indirizzi assoluti	
Scrittura di variabili tramite indirizzo assoluto	Applet: Scrittura di variabili tramite indirizzi assoluti	
Accesso ai file nella stazione S7 con FTP	FTP: Lettura dei file (DB) dalla CPU S7	
	FTP: Scrittura dei file (DB) nella CPU S7	
	FTP: Lettura dei file dal sistema di file CP	Sistema di file
	FTP: Scrittura dei file sul sistema di file CP	
	Web: Formattazione del sistema di file CP	
Invio di una mail di test tramite la pagina del sistema	Web: Accesso alla diagnostica Web e al sistema di file CP	Web
	Web: Invio di una mail di test	
Interrogazione dello stato di unità	Applet: Lettura dello stato delle unità nel rack	SPS
Interrogazione dei numeri di ordinazione delle unità	Applet: Lettura del numero di ordinazione delle unità nel rack	

Vedere anche

Sincronizzazione dell'ora (Pagina 185)

Progettazione dell'elenco degli accessi (Pagina 117)

2.4.4 Informazioni generali

Contenuti generali

Sia nella versione Standalone del Security Configuration Tool sia nella versione integrata in STEP 7, durante la creazione di un nuovo progetto viene richiesto di inserire un nome utente e una password. L'utente che viene creato è del tipo "administrator". Dopo l'inserimento è possibile eseguire le configurazioni nel progetto.

Le configurazioni di un progetto contengono in generale:

- Impostazioni valide in tutto il progetto
- Impostazioni specifiche per l'unità
- Assegnazione ai gruppi per tunnel IPsec S602

Inoltre una gestione utenti regola le autorizzazioni di accesso ai dati del progetto e alle unità Security.

Impostazioni valide in tutto il progetto

- Proprietà del progetto

  Oltre all'indicazione di indirizzo e di nome, queste proprietà comprendono indicazioni per i valori di inizializzazione.

- Set di regole firewall globali

  Un set di regole firewall globale può essere assegnata contemporaneamente a diverse unità Security. In molti casi questa possibilità semplifica la progettazione rispetto alla progettazioni di regole firewall nelle impostazioni specifiche per l'unità.

- Set di regole IP personalizzati S≥V3.0

  Un set di regole IP personalizzato viene assegnato ad un utente e ad un'unità Security. Ad un'unità SCALANCE S V4 può essere assegnato anche un set di regole IP personalizzato al quale è assegnato un ruolo.

  I set di regole IP personalizzati consentono la definizione di diritti di accesso capillari, specifici per l'utente.

- Relazioni di ridondanza S62x ≥ V4.0

  Una relazione di ridondanza viene creata per due unità Security. Se una delle due unità Security si guasta durante il funzionamento, l'altra unità Security assume automaticamente la sua funzione di firewall e router (NAT/NAPT).

- Domini MRP S627-2M

  Con i domini MRP vengono definiti i nodi di un anello MRP. Per le interfacce di tutte le unità che devono essere collegate ad un anello MRP è necessario selezionare lo stesso dominio MRP.

- Definizione del servizio

  Grazie alla definizione di servizi IP o MAC è possibile definire in modo chiaro e compatto le regole del firewall.

- Server NTP

  I server NTP vengono progettati per tutto il progetto e possono quindi essere assegnati a diverse unità Security nell'SCT.

- Server RADIUS S≥V4.0

  I server RADIUS vengono progettati per tutto il progetto e possono quindi essere assegnati a diverse unità Security nell'SCT.

- Manager dei certificati

  Nel manager dei certificati vengono gestiti tutti i certificati del progetto e delle unità ivi contenuti.

- Gestione utenti

  Nella gestione utenti possono essere gestiti tutti gli utenti del progetto e i relativi diritti nonché essere definite le direttive password.

- Nome simbolico

  In un progetto al posto di indirizzi IP e indirizzi MAC è possibile assegnare nomi simbolici in una tabella.

Impostazioni specifiche per l'unità

La maggior parte di funzioni vengono configurate nelle schede della finestra di dialogo delle proprietà che può essere richiamata per un'unità Security selezionata tramite la voce di menu "Modifica " > "Proprietà...". Nella finestra di dialogo delle proprietà è possibile ordinare a piacere le singole finestre tramite Drag & Drop. Nella seguente tabella sono illustrate le descrizioni delle funzioni delle singole schede.

	Funzione / scheda nella finestra di dialogo delle proprietà	disponibile nella modalità …	
		Standard	estesa
	Interfacce Panoramica delle singole impostazioni delle interfacce e delle porte. Per CP: Le impostazioni vengono acquisite da STEP 7 e non possono essere modificate.	X	X
	Firewall Nella modalità standard attivare il firewall con semplici regole standard. Inoltre è possibile attivare le impostazioni Log. Nella modalità estesa è possibile definire regole del filtro pacchetto dettagliate. Inoltre è possibile definire impostazioni di log esplicite per ogni regola del filtro pacchetto. Per CP: Se è stato migrato un elenco Access Control, esso viene qui visualizzato e può essere modificato.	X	X
S≥V3.0	**Collegamento Internet** Se è impostato un collegamento tramite PPPoE eseguire qui le impostazioni per l'Internet Service Provider.	X	X
S≥V3.0	**DNS** Impostazioni per DNS dinamico che consentono l'accesso a indirizzi IP che variano costantemente tramite nomi definiti in modo fisso (FQDN). Il DNS dinamico è ammesso sull'interfaccia esterna e sull'interfaccia DMZ.	-	X

	Funzione / scheda nella finestra di dialogo delle proprietà	disponibile nella modalità …	
		Standard	estesa
	Routing Inserire qui i dati relativi al router standard e/o definire un instradamento specifico per la rete. Per CP: L'indicazione di un router standard viene rilevata da STEP 7 e può essere modificata solo in STEP 7. La visualizzazione avviene nell'area del contenuto dell'SCT. Di conseguenza la scheda non è presente nelle proprietà del modulo.	X	X
	NAT/NAPT Attivare la funzionalità NAT/NAPT e definire la conversione di indirizzi in un elenco.	-	X
	Sincronizzazione dell'ora Definire il tipo di sincronizzazione per data e ora. Per CP: La sincronizzazione dell'ora può essere configurata nell'SCT solo se in STEP 7 è stata attivata la configurazione NTP estesa.	X	X
	Impostazioni Log Qui è possibile eseguire indicazioni più esatte relative alla modalità di registrazione e di salvataggio di eventi log e progettare la trasmissione ad un server Syslog.	-	X
	VPN Se l'unità Security si trova in un gruppo VPN, qui è possibile configurare la Dead-Peer-Detection, il tipo di realizzazione del collegamento ed eventualmente un punto di accesso WAN (indirizzo IP o FQDN). In base all'unità Security eseguire nel campo della finestra di dialogo le impostazioni relative alle sotto-reti, ai nodi IP/MAC e ai nodi NDIS, alle quali è possibile accedere anche tramite i tunnel VPN. Per SCALANCE S: L'apprendimento di nodi interni può essere attivato o disattivato. Il campo della finestra di dialogo "Nodi VPN" viene visualizzata solo se il progetto si trova in modalità estesa.	X	X
	Server DHCP Per la rete interna e per la rete DMZ (solo SCALANCE S623/S627-2M) è possibile utilizzare l'unità Security come server DHCP.	-	X
	SNMP Impostare in questa scheda la versione di protocollo SNMP e il metodo di autenticazione/codifica.	X	X
	Proxy ARP Impostare in questa scheda le voci statiche per Proxy ARP sull'interfaccia esterna.	-	X
	MRP/HRP Impostare in questa scheda i parametri per il collegamento dell'unità Security agli anelli MRP/HRP.	X	X

	Funzione / scheda nella finestra di dialogo delle proprietà	disponibile nella modalità …	
		Standard	estesa
S≥V4.0	**RADIUS** Assegnare all'unità Security in questa scheda un server RADIUS che autentica gli utenti durante l'attivazione dei set di regole IP personalizzati al posto dell'unità Security.	X	X

Assegnazione ai gruppi per tunnel VPN

S602

I gruppi VPN definiscono quali unità Security, SOFTNET Security Client e unità SCALANCE M, dispositivi VPN e client VPN NCP (Android) devono comunicare tra loro tramite tunnel IPsec.

Assegnando questo nodo di rete ad un gruppo VPN è possibile realizzare un tunnel di comunicazione tramite una VPN (Virtual Private Network).

Solo le unità dello stesso gruppo VPN possono comunicare tra loro in modo protetto tramite tunnel, per cui le unità possono far parte simultaneamente di diversi gruppi VPN.

Vedere anche

Progettazione di ulteriori proprietà dell'unità (Pagina 163)

2.4.5 Definizione dei valori di inizializzazione standard per un progetto

SR

Definizione dei valori di inizializzazione standard per un progetto

Con i valori di inizializzazione standard si definiscono le proprietà che vengono riprese automaticamente durante la creazione di nuove unità. Dalla casella di controllo "Salva selezione" definire inoltre se durante la creazione di una nuova unità deve aprirsi una finestra per l'impostazione delle proprietà o se l'unità viene inserita direttamente.

Selezionare la voce di menu "Progetto" > "Proprietà...", scheda "Valori di inizializzazione standard"

Protezione dei dati del progetto tramite codifica

I dati del progetto e di configurazione salvati sono protetti sia nel file del progetto, sia nel C-PLUG (non per CP 1628) tramite codifica.

2.4.6 Controlli di coerenza

Informazioni generali

Security Configuration Tool distingue:

- Controlli di coerenza locali
- Controlli di coerenza in tutto il progetto

Per maggiori informazioni sulle regole da osservare durante l'immissione, consultare le relative descrizioni delle finestre di dialogo riportate alla voce "Controllo della coerenza".

Controlli di coerenza locali

Un controllo della coerenza è definito locale quando si può eseguire direttamente all'interno di una finestra di dialogo. Con le seguenti azioni possono essere eseguiti controlli:

- dopo essere usciti da un campo
- dopo essere usciti da una riga in una tabella
- uscendo dalla finestra di dialogo con "OK"

Controlli di coerenza in tutto il progetto

I controlli della coerenza in tutto il progetto forniscono informazioni sulle unità configurate correttamente. Nelle seguenti azioni viene eseguito un controllo automatico della coerenza su tutto il progetto:

- durante il salvataggio del progetto
- durante l'apertura del progetto
- prima del caricamento di una configurazione

Nota

I dati di progettazione possono essere caricati solo se il progetto è complessivamente coerente.

Per eseguire un controllo della coerenza in tutto il progetto, procedere nel modo seguente

Eseguire il controllo della coerenza per un progetto aperto nel modo seguente:

Voce di menu: "Opzioni" > "Controlli della coerenza...".

Il risultato del controllo viene visualizzato in un elenco che può essere filtrato a seconda del tipo di messaggio "Errori" o "Avvertimenti". Se il progetto contiene dati incoerenti, lo stato viene visualizzato nella riga di stato della finestra SCT. Fare clic sulla riga di stato per visualizzare l'elenco di controllo.

2.4.7 Impostazione di nomi simbolici per indirizzi IP/MAC.

A questa funzione si accede nel modo seguente

Voce di menu: "Opzioni" > "Nomi simbolici ...".

Significato e vantaggio

In un progetto Security al posto di indirizzi IP e indirizzi MAC è possibile assegnare nomi simbolici in una tabella.

La progettazione dei singoli servizi può quindi essere eseguita in modo più semplice e sicuro.

Per le seguenti funzioni e relativa progettazione vengono tenuti in considerazione nomi simbolici all'interno di un progetto:

- Firewall
- Router NAT/NAPT
- Syslog
- DHCP
- NTP

Formazione di nomi simbolici

Il nome simbolico deve essere preimpostato sia durante la definizione sia in caso di utilizzo di un carattere cancelletto (#). I nomi simbolici stessi devono essere conformi a DNS.

Validità e univocità

La validità dei nomi simbolici indicati nella tabella è limitata alla progettazione all'interno di un progetto Security.

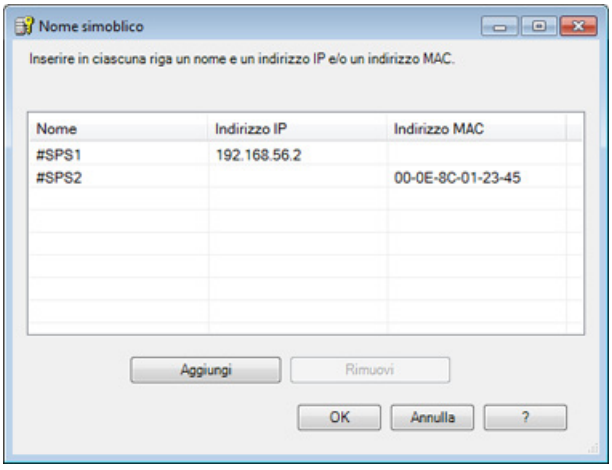
All'interno del progetto ad ogni nome simbolico deve essere assegnato in modo univoco un solo indirizzo IP e/o indirizzo MAC.

Finestra di dialogo per la definizione di nomi simbolici

Per evitare incoerenze tra un'assegnazione "Indirizzo IP - nome simbolico" e "Indirizzo MAC - nome simbolico", i nomi simbolici vengono gestiti in una singola tabella.

Definizione di nomi simbolici

1. Azionare il pulsante "Aggiungi" per inserire un nuovo nome simbolico nella successiva riga libera della tabella.
2. Inserire un carattere cancelletto (#) seguito dal nome simbolico desiderato conforme a DNS.
3. Completare la voce con l'indirizzo IP e/o l'indirizzo MAC.



Utilizzo di nomi simbolici non definiti

Nell'ambito della progettazione di unità Security è possibile utilizzare anche nomi simbolici che non sono ancora definiti. Dopo l'inserimento di un nome simbolico non ancora definito e la conferma della relativa finestra di dialogo, il nome simbolico selezionato viene inserito nella tabella dei nomi simbolici. In questa finestra di dialogo è quindi possibile definire il relativo indirizzo IP e/o indirizzo MAC per nomi simbolici.

Se si cancella una voce dalla tabella, i nomi simbolici utilizzati nei servizi vengono mantenuti. In questo caso il controllo della coerenza riconosce i nomi simbolici non definiti. Questo vale indipendentemente dal fatto che si sia definito o meno il nome simbolico in seguito.

Suggerimento:

Per la tabella qui descritta è particolarmente sensato l'impiego del controllo della coerenza in tutto il progetto. In base all'elenco si possono riconoscere e correggere incoerenze.

Avviare il controllo della coerenza per un progetto aperto con la voce di menu "Opzioni" > "Controlli della coerenza...".

Controllo della coerenza - vanno osservate queste regole

Per l'inserimento rispettare le regole riportate qui di seguito:

- Il nome simbolico deve essere preceduto da un carattere cancellato (#).
- L'assegnazione di un nome simbolico ad un indirizzo IP o ad un indirizzo MAC deve essere univoco. Il nome simbolico e l'indirizzo devono essere inseriti una sola volta e non devono essere utilizzati in un'altra voce dell'elenco.
- I nomi simbolici devono essere conformi a DNS.

- Ad un nome simbolico deve essere assegnato un indirizzo IP, un indirizzo MAC o entrambi gli indirizzi.
- Agli indirizzi IP dell'unità Security non devono essere assegnati nomi simbolici.
- I nomi simbolici utilizzati nel progetto per gli indirizzi IP o gli indirizzi MAC devono essere trovarsi nella tabella.

  Possono verificarsi incoerenze dovute alla cancellazione delle voci nella tabella e alla mancata relativa cancellazione o correzione nelle finestre di dialogo di progettazione.

Vedere anche

Controlli di coerenza (Pagina 61)

Conformità DNS (Pagina 263)

2.5 Gestione degli utenti

2.5.1 Panoramica della gestione utenti

Com'è strutturata la gestione utenti?

L'accesso alla configurazione Security viene gestito con le impostazioni utente configurabili. Configurare gli utenti con rispettivamente una password per l'autenticazione. Assegnare ad un utente un ruolo definito dal sistema o dall'utente. Ai ruoli sono assegnati diritti specifici per la progettazione o per l'unità. Durante la creazione fare attenzione alle strutture d'insieme (Pagina 20) indicate.

Migrazione di utenti già esistenti da STEP 7 a SCT

S7-CP

Gli utenti già creati in STEP 7 possono essere migrati nell'SCT. In questo caso è necessario riassegnare le password.

Le informazioni dettagliate su questo argomento si trovano nella guida in linea.

Alla guida è possibile accedere con il tasto F1 o con il pulsante "Help" nella relativa finestra di dialogo SCT.

Sequenza di inserimento durante la creazione di utenti e di ruoli

Selezionare una delle due sequenze di inserimento:

- Creare dapprima un nuovo utente, definire quindi un ruolo e assegnare infine il ruolo all'utente.
- Definire dapprima un nuovo ruolo, creare quindi un utente e assegnare infine il ruolo all'utente.

Nota

Custodire le password utente in modo sicuro.

Se si dimenticano le password utente, non si dispone più dell'accesso al progetto interessato o alle unità Security interessate.

In questo caso è necessario creare un nuovo progetto ed eseguire un "Reset alle impostazioni di fabbrica". In questo caso di perdono però le configurazioni.

Nota

Se si modificano le impostazioni di autenticazione, è necessario caricare di nuovo prima le unità Security in modo che queste impostazioni (ad es. nuovi utenti, modifiche di password) diventino attive nelle unità Security.

Autenticazione utenti durante l'attivazione di set di regole IP personalizzati S≥V3.0

L'autenticazione di utenti che si connettono alla pagina Web dell'unità Security per attivare un set di regole IP personalizzato può essere eseguita dall'unità Security o da un server RADIUS.

La definizione del metodo di autenticazione "RADIUS" per un utente è descritta nel seguente capitolo:

- Crea utente (Pagina 66)

Le informazioni dettagliate sull'autenticazione utente mediante server RADIUS si trova nel seguente capitolo:

- Autenticazione mediante server RADIUS (Pagina 75)

2.5.2 Crea utente

A questa funzione si accede nel modo seguente

Voce di menu SCT: "Opzioni" > "Gestione utenti...", scheda "Utenti", pulsante "Aggiungi...".

Voce di menu STEP 7: "Utenti" > "Avvio della gestione utenti", pulsante "Esegui". Inoltre la gestione utenti può essere richiamata da singole schede.

Parametri	Significato
Nome utente	Nome utente liberamente selezionabile.
Metodo di autenticazione	• **Password**: Utilizzare questo metodo di autenticazione per utenti che devono modificare e caricare il progetto SCT nonché diagnosticare l'unità Security. L'autenticazione dell'utente viene eseguita durante l'attivazione dei set di regole IP personalizzate mediante l'unità Security. • **RADIUS** S≥V4.0 : L'autenticazione dell'utente viene eseguita durante l'attivazione dei set di regole IP personalizzate mediante il server RADIUS. Con questo metodo di autenticazione la password dell'utente non viene progettata in SCT, ma deve essere memorizzata sul server RADIUS. Utilizzare questo metodo di autenticazione esclusivamente per utenti che devono connettersi solo a questa pagina Web di un'unità Security. Un utente con metodo di autenticazione "RADIUS" non può connettersi ai progetti SCT.
Password (solo con il metodo di autenticazione "Password")	Inserimento della password per l'utente. Durante l'inserimento viene controllata la complessità della password. Maggiori informazioni relative alla complessità della password si trovano nel seguente capitolo: Regole per nome utente, ruoli e password (Pagina 21)
Ripeti password (solo con il metodo di autenticazione "Password")	Ripetizione della password inserita.
Commento	Inserimento supplementare di un commento.
Durata massima della sessione S≥V3.0	Inserimento della durata dopo la quale viene disconnesso automaticamente un utente collegato alla pagina Web per i set di regole IP personalizzati delle unità SCALANCE S. La durata qui indicata inizia dopo la connessione e dopo una nuova sessione alla pagina Web dell'unità Security. • Impostazione standard: 30 minuti • Valore minimo: 5 minuti • Valore massimo: 480 minuti
Ruolo assegnato	A seconda dell'assegnazione eseguita.

Tabella 2- 1 Pulsante nella scheda "Utenti"

Denominazione	Significato / Effetto
Modifica...	Selezionare una voce e fare clic sul pulsante. Nella finestra di dialogo evidenziata si modificano le impostazioni riportate sopra.
Aggiungi...	Aggiungere un nuovo utente con il pulsante.
Del	Cancellare la voce selezionata con il pulsante. **Avvertenza** Nel progetto deve sempre essere presente almeno un utente con il ruolo "Amministratore". L'amministratore creato automaticamente durante la realizzazione del progetto può essere cancellato solo se esiste almeno un altro utente con diritti di progettazione completi.

2.5.3 Creazione dei ruoli

Quali ruoli esistono?

Ad un utente può essere assegnato un ruolo definito dal sistema o dall'utente. I diritti dell'unità di un ruolo ruoli definito dall'utente si definisce per ogni unità Security.

Ruoli definiti dal sistema

Sono predefiniti i seguenti ruoli definiti dal sistema. Ai ruoli sono assegnati determinati diritti uguali su tutte le unità e che non possono essere modificati o cancellati dall'amministratore.

Gestione dei diritti (Pagina 69)

- administrator

  Ruolo standard per la creazione di un nuovo progetto SCT.

  Diritti di accesso illimitati ai tutti i dati di configurazione.

- standard

  Ruolo con diritti di accesso limitati.

- diagnostics

  Ruolo standard per la creazione di un nuovo utente.

  Accesso solo in lettura.

- remote access

  Nessun diritto tranne connessione alla pagina Web per set di regole IP personalizzate.

- radius

  Ruolo che può essere utilizzato per l'attivazione di set di regole IP personalizzate.

  Accesso solo in lettura.

- administrator (radius)

  Ruolo che può essere utilizzato per l'attivazione di set di regole IP personalizzate.

  Diritti d'accesso ai dati di configurazione tranne ai MIB SNMP.

Nota

Ulteriori informazioni relative ai set di regole IP personalizzate si trovano nel seguente capitolo:

Set di regole IP specifiche per l'utente (Pagina 138)

Nota

Ulteriori informazioni relative all'autenticazione tramite server RADIUS si trovano nel seguente capitolo:

Autenticazione mediante server RADIUS (Pagina 75)

Ruolo definito dall'utente

Oltre ai ruoli definiti dal sistema possono essere creati ruoli definiti dall'utente. Per un ruolo definito dall'utente selezionare i diritti di progettazione e dell'unità e definire i diritti corrispondenti per ciascuna unità Security utilizzata nel progetto. Assegnare manualmente i ruoli definiti dall'utente all'utente corrispondente.

A questa funzione si accede nel modo seguente

Voce di menu SCT: "Opzioni" > "Gestione utenti...", scheda "Ruoli".

Voce di menu STEP 7: "Utenti" > "Avvio della gestione utenti", pulsante "Esegui". Inoltre la gestione utenti può essere richiamata da singole schede.

Tabella 2- 2 Indicazioni nella scheda "Ruoli"

Parametri	Significato
Nome ruoli	Nome ruolo liberamente selezionabile.
Commento	Inserimento supplementare di un commento.
Durata massima della sessione S≥V3.0	Inserimento della durata dopo la quale viene disconnesso automaticamente un utente con il ruolo assegnato connesso alla pagina Web per i set di regole IP personalizzati delle unità SCALANCE S. La durata qui indicata inizia dopo la connessione e dopo una nuova sessione alla pagina Web dell'unità Security. • Impostazione standard: 30 minuti • Valore minimo: 5 minuti • Valore massimo: 480 minuti

Tabella 2- 3 Pulsante nella scheda "Ruoli"

Denominazione	Significato / Effetto
Proprietà... / Modifica...	Selezionare un ruolo definito dall'utente nell'elenco e fare clic sul pulsante. Nella finestra di dialogo evidenziata si modificano le proprietà del ruolo, quali il nome di ruolo, i diritti assegnati al ruolo e la durata massima della sessione. I ruoli definiti dal sistema non possono essere modificati.
Aggiungi...	Aggiungere un nuovo ruolo definito dall'utente con il pulsante. Inserire nella finestra di dialogo evidenziata il nome del ruolo e assegnare i diritti corrispondenti al ruolo dell'elenco dei diritti. Vengono visualizzati i diritti del ruolo definito dal sistema selezionato nel modello dei diritti (indicazioni standard: "diagnostics").
Del	Cancellare la voce selezionata con il pulsante. **Avvertenza** • Un ruolo definito dall'utente già creato può essere cancellato solo se non è assegnato a nessun utente. Assegnare eventualmente all'utente un altro ruolo. • I ruoli definiti dal sistema non possono essere cancellati.

2.5.4 Gestione dei diritti

A questa funzione si accede nel modo seguente

Voce di menu SCT: "Opzioni" > "Gestione utenti...", scheda "Ruoli", pulsante "Proprietà…" e "Aggiungi…".

Voce di menu STEP 7: "Utenti" > "Avvio della gestione utenti", pulsante "Esegui". Inoltre la gestione utenti può essere richiamata da singole schede.

Creazione e assegnazione del ruolo definito dall'utente

1. Inserire un nome di ruolo.
2. Selezionare un ruolo definito dal sistema dal modello dei diritti (indicazione standard: "diagnostics"). I ruoli definiti dall'utente non vengono visualizzati nella selezione.

   Risultato: In base al ruolo selezionato per ciascuna unità Security utilizzata nel progetto vengono visualizzati i relativi ruoli nell'elenco dei diritti. I diritti delle unità Security non utilizzati nel progetti sono visualizzati in grigio.
3. Attivare o disattivare per ciascuna unità Security i diritti che devono essere assegnati al ruolo definito dall'utente.
4. Inserire eventualmente un commento e una lunghezza massima della sessione per il ruolo da creare.

5. Fare clic sul pulsante "Acquisisci" per salvare la selezione o su "OK" per salvare e chiudere la finestra.
6. Assegnare il ruolo ad un utente.

Copia del diritti del ruolo di un'unità Security

Selezionare nel menu contestuale di un'unità Security dall'elenco degli oggetti il comando "Copia diritti..." e assegnarlo tramite il comando "Inserisci diritti..." ad un'altra unità Security.

Diritti di progettazione

A seconda del tipo di ruolo per ciascun progetto Security possono essere selezionati i seguenti diritti di progettazione:

Tabella 2- 4 Diritti di progettazione per l'accesso al progetto Security

Diritto di progettazione	administrator	standard	diagnostics
Diagnostica della Security	x	x	x
Configurazione della Security	x	x	-
Gestione utenti e ruoli	x	-	-

x il diritto è attivato

- il diritto è disattivato

Diritti dell'unità

Nella colonna "Servizio" viene visualizzato il sistema sul quale ha effetti il rispettivo diritti.

A seconda del tipo di ruolo per ciascun progetto Security possono essere selezionati i seguenti diritti dell'unità:

Tabella 2- 5 Diritti dell'unità CP x43-1 Adv.

Diritto all'interno del servizio	administrator	standard	diagnostics	Servizio
Web: Formattazione del sistema di file CP *	x	-	-	Sistema di file
FTP: Lettura dei file dal sistema di file CP	x	x	x	
FTP: Scrittura dei file sul sistema di file CP	x	x	-	
FTP: Lettura dei file (DB) dalla CPU S7 **	x	x	x	SPS
FTP: Scrittura dei file (DB) nella CPU S7 ***	x	x	-	
Applet: Lettura di variabili tramite i simboli progettati *	x	x	x	
Applet: Scrittura di variabili tramite i simboli progettati *				
Applet: Lettura di variabili tramite indirizzi assoluti *	x	x	x	
Applet: Scrittura di variabili tramite indirizzi assoluti *	x	x	-	
Applet: Lettura dello stato delle unità nel rack *	x	x	x	
Applet: Lettura del numero di ordinazione delle unità nel rack *	x	x	x	
SNMP: Lettura MIB-II	x	x	x	SNMP
SNMP: Scrittura MIB-II	x	x	-	
SNMP: Lettura MIB di automazione	x	x	x	
SNMP: Lettura MIB LLDP	x	x	x	
SNMP: Lettura MIB SNMPv2	x	x	x	
SNMP: Lettura MIB MRP	x	x	x	
SNMP: Scrittura MIB MRP	x	x	-	
SCT: Esecuzione della diagnostica dell'unità Security ****	x	x	x	Sicurezza
Web: Estensione dell'elenco IP Access Control *	x	-	-	
Web: Accesso alla diagnostica Web e al sistema di file CP	x	x	x	Web
Web: Invio di una mail di test *	x	x	x	
Web: Aggiornamento del firmware *	x	x	-	Manutenzione
Web: Caricamento successivo di testi della diagnostica *	x	x	-	

x il diritto è attivato

- il diritto è disattivato

* Per utilizzare la funzione deve essere attivato il diritto dell'unità "Web: Accesso alla diagnostica Web e al sistema di file CP".

** Per utilizzare la funzione deve essere attivato anche il diritto dell'unità "FTP: Lettura dei file dal sistema di file CP".

*** Per utilizzare la funzione deve essere attivato anche il diritto dell'unità "FTP: Scrittura dei file nel sistema di file CP".

**** Per utilizzare la funzione deve essere attivato anche il diritto di progettazione "Diagnostica Security".

Tabella 2- 6 Diritti dell'unità del CP 1628:

Diritto all'interno del servizio	administrator	standard	diagnostics	Servizio
SNMP: Lettura MIB-II	x	x	x	SNMP
SNMP: Scrittura MIB-II	x	x	-	
SNMP: Lettura MIB di automazione	x	x	x	
SNMP: Lettura MIB SNMPv2	x	x	x	
SCT: Esecuzione della diagnostica dell'unità Security	x	x	x	Sicurezza

x il diritto è attivato

- il diritto è disattivato

Tabella 2- 7 Diritti dell'unità SCALANCE S ≥ V3.0

Diritto all'interno del servizio	administrator	standard	diagnostics	Servizio
SNMP: Lettura MIB-II	x	x	x	SNMP
SNMP: Scrittura MIB-II	x	x	-	
SNMP: Lettura MIB di automazione	x	x	x	
SNMP: Lettura MIB SNMPv2	x	x	x	
SNMP: Lettura MIB MRP S627-2M	x	x	x	
SNMP: Scrittura MIB MRP S627-2M	x	x	-	
SCT: Esecuzione della diagnostica dell'unità Security	x	x	x	Sicurezza
Caricamento dei file di configurazione	x	x	-	
Web: Aggiornamento del firmware	x	x	-	Manuten-zione

x il diritto è attivato

- il diritto è disattivato

Tabella 2- 8 Diritti dell'unità SCALANCE S < V3.0

Diritto all'interno del servizio	administrator	standard	diagnostics	Servizio
Caricamento dei file di configurazione	x	x	-	Sicurezza
SCT: Esecuzione della diagnostica dell'unità Security	x	x	x	

x il diritto è attivato

- il diritto è disattivato

Impostazione dei diritti dell'unità prima e dopo la creazione di unità Security

All'interno di un ruolo definito dall'utente i diritti dell'unità vengono definiti separatamente per ciascuna unità Security. Se prima di aggiungere il ruolo è stata creata un'unità Security per la quale devono essere definiti diritti dell'unità all'interno di un ruolo, i diritti dell'unità vengono impostati automaticamente per questa unità Security in base al ruolo definito selezionato e, in caso di necessità, possono essere adattati. Se dopo la creazione di un ruolo è stata aggiunta un'unità Security, SCT non imposta nessun diritto. In questo caso è necessario impostare tutti i diritti di unità per l'unità Security stessa.

I diritti dell'unità già esistenti possono anche essere acquisiti in un'altra unità Security mediante copiatura e da qui essere eventualmente modificati. Selezionare quindi nel menu di scelta rapida di un'unità Security, nei diritti dell'unità la voce di menu "Copia diritti..." o "Inserisci diritti...".

2.5.5 Progettazione delle direttive password

Significato

Con le direttive password è possibile stabilire predefinizioni che devono essere osservate durante l'assegnazione di password al nuovo utente.

A questa funzione si accede nel modo seguente

Selezionare la voce di menu "Opzioni" > "Gestione utenti...", scheda "Direttive password". Dopo l'attivazione di una casella di controllo la rispettiva direttiva è attiva e può eventualmente essere adattata tramite la relativa casella di inserimento.

Parametri	Significato
Lunghezza minima della password	Numero di caratteri minimo che devono contenere le password. Come standard la rispettiva casella di controllo è attivata e non può essere disattivata. • Valore minimo: 8 caratteri • Valore massimo: 32 caratteri
Numero minimo di cifre	Numero minimo di cifre che devono contenere le password. • Valore minimo: 1 cifra • Valore massimo: 32 cifre
Numero minimo di caratteri speciali	Numero di caratteri speciali che devono contenere le password. Un carattere speciale è ciascun carattere che non è né una lettera né una cifra. • Valore minimo: 1 carattere speciale • Valore massimo: 32 carattere speciale

Parametri	Significato
Numero di password bloccate per il riutilizzo	Numero delle password utilizzate per ultime che non sono disponibili come nuove password per una modifica di password. • Valore minimo: 1 password • Valore massimo: 10 password
Almeno una lettera maiuscola e una lettera minuscola	Se si attiva questa casella di controllo, le password devono contenere almeno una lettera maiuscola e una lettera minuscola.

2.5.6 Autenticazione mediante server RADIUS

2.5.6.1 Informazioni generali

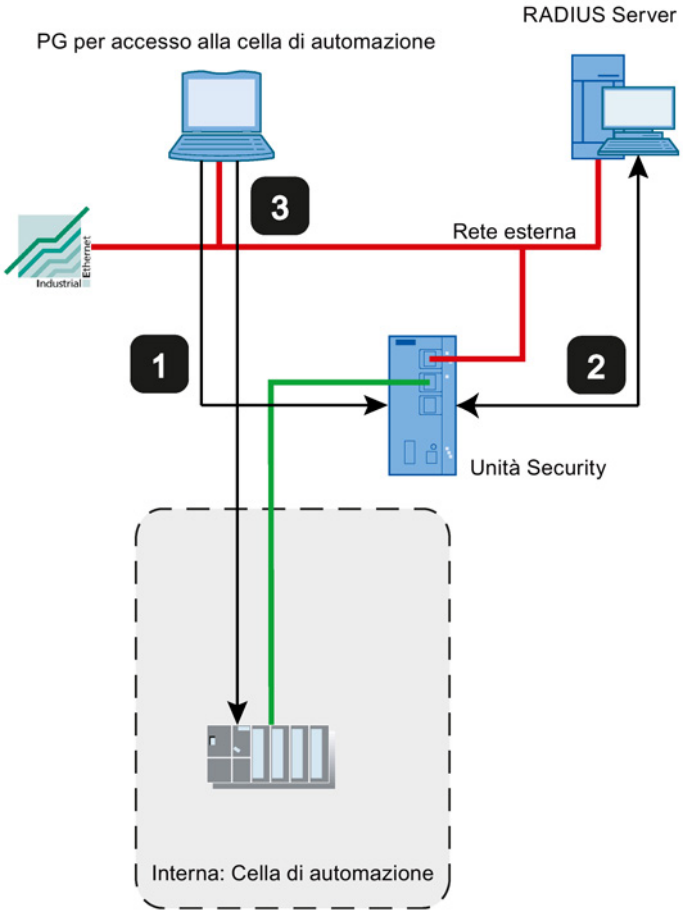
S≥V4.0

Significato

RADIUS (Remote Authentication Dial-In User Service) è un protocollo per l'autenticazione di utenti mediante server sui quali possono essere memorizzati dati utente. Impiegando server RADIUS è possibile aumentare la protezione di nomi utente, ruoli e password assegnati.

Settore d'impiego di server RADIUS

L'autenticazione mediante server RADIUS può essere eseguita nell'ambito dell'attivazione dei set di regole IP personalizzati.



1 Inserimento dei dati utente nella pagina Web dell'unità Security
2 Autenticazione mediante server RADIUS e attivazione del set di regole IP personalizzato
3 Accesso alla cella di automazione

La configurazione di rete illustrata sopra rappresenta un esempio. Il server RADIUS può trovarsi anche nella rete interna o nella rete DMZ dell'unità Security.

Per le possibilità di progettazione descritte di seguito il presupposto è che sia progettato un server RADIUS in SCT e che la relativa unità Security sia stata assegnata. Inoltre un utente o un ruolo deve essere progettato con il metodo di autenticazione "RADIUS". Informazioni su questo argomento si trovano nel seguente capitolo:

- Definizione del server ADIUS (Pagina 78)
- Assegnazione del server RADIUS ad un'unità Security (Pagina 79)
- Crea utente (Pagina 66)
- Creazione dei ruoli (Pagina 67)

Ulteriori generali relative ai set di regole IP personalizzate si trovano nel seguente capitolo:

- Set di regole IP specifiche per l'utente (Pagina 138)

Possibilità di progettazione

Per l'autenticazione dell'utente mediante un server RADIUS sono disponibili due possibilità di progettazione:

- L'utente è conosciuto con il suo ruolo sull'unità Security, solo la gestione della password per l'utente viene eseguita tramite il server RADIUS. Sul server RADIUS è configurato l'utente con la password corrispondente.
  - Viene progettato un utente con il metodo di autenticazione "RADIUS".
  - Al set di regole IP personalizzate viene assegnato l'utente.

  Risultato:
  - Durante la connessione di un utente alla pagina Web dell'unità Security, la richiesta di autenticazione viene inoltrata al server RADIUS.
  - Il server RADIUS esegue una verifica della password e invia il risultato all'unità Security.
  - Se la verifica della password è stata superata, il set di regole IP personalizzato viene attivato.
- Il ruolo è conosciuto sull'unità Security, la gestione utenti viene eseguita tramite il server RADIUS. Sul server RADIUS è configurato l'utente con la password corrispondente.
  - Al set di regole IP personalizzato viene assegnato un ruolo personalizzato o un ruolo definito dal sistema.
  - Nella scheda "RADIUS" dell'unità Security viene viene attivata la casella di controllo "Consenti autenticazione RADIUS a utenti non progettati" e la casella di controllo "L'ID filtro è necessario per l'autenticazione".

  Risultato:
  - Durante la connessione di un utente alla pagina Web dell'unità Security, la richiesta di autenticazione e di autorizzazione viene inoltrata al server RADIUS.
  - Il server RADIUS esegue una verifica della password e invia il risultato all'unità Security.

- Caso a: Se inoltre è progettato il nome del ruolo sul server RADIUS:

  Il server RADIUS restituisce il nome di ruolo assegnato all'utente all'unità Security.
- Caso b: Se il nome del ruolo non è progettato sul server RADIUS:

  L'unità Security assegna all'utente il ruolo definito dal sistema "radius".
- Se la verifica della password è stata superata, il set di regole IP personalizzato viene attivato.

Accordi per server RADIUS

- I server RADIUS possono trovarsi in ciascuna rete collegata all'unità Security.
- Per ciascuna unità Security possono essere progettati al massimo due server RADIUS. Durante il funzionamento è quindi attivo solo uno dei server RADIUS.
- Per la definizione di un server RADIUS al posto di un indirizzo IP è possibile utilizzare anche un FQDN.

2.5.6.2 Definizione del server ADIUS

S≥V4.0

Significato

Prima che l'autenticazione possa essere eseguita mediante un server RADIUS, esso deve essere dapprima memorizzato nel progetto SCT. Infine è necessario assegnare il server RADIUS definito all'unità Security per la quale il server RADIUS deve acquisire l'autenticazione utente.

Procedimento

1. Selezionare la voce di menu "Opzioni" > "Configurazione del server RADIUS...".
2. Fare clic sul pulsante "Aggiungi...".
3. Inserire il parametri necessari in base alla seguente tabella.

Parametri	Significato
Nome	Nome a scelta per il server RADIUS.
Indirizzo IP / FQDN	Indirizzo IP o FQDN del server RADIUS.
Porta	Porta UDP alla quale è raggiungibile il server RADIUS. Come standard vengono ricevuti dati di autenticazione sulla porta 1812.
Shared Secret	Inserimento della password che viene utilizzata per la codifica durante la trasmissione dei dati di connessione tra il server RADIUS e l'unità Security. Sono consentiti i seguenti caratteri del set di caratteri ANSI X 3.4-1986: 0123456789 A...Z a...z !#$%&()"*'+`,-./:;<=>?@ [\]_{|}~^ Lunghezza del Shared-Secret: 1 ... 31 caratteri
Ripetizione di Shared Secret	Conferma della password.
Metodo di autenticazione	Indicazione del procedimento che viene utilizzato per il controllo dei dati utente. Viene supportato solo il procedimento "PAP" (Password Authentication Protocol).
Commento	Inserimento opzionale a scelta.

Risultato

È stato definito un server RADIUS ed esso può essere assegnato solo alle unità Security desiderate.

2.5.6.3 Assegnazione del server RADIUS ad un'unità Security

S≥V4.0

Requisito richiesto

È stato definito un server RADIUS.

Procedimento

1. Selezionare l'unità Security che si vuole assegnare ad un server RADIUS.
2. Selezionare la voce di menu "Modifica" > "Proprietà...".
3. Selezionare la scheda "RADIUS".
4. Attivare la casella di controllo "Attiva autenticazione RADIUS".

   Nota

   Modifica del metodo per l'autenticazione con Webserver sull'unità Security

   Se viene attivata l'autenticazione RADIUS sull'unità Security, il metodo di autenticazione con il Webserver viene commutato da "Digest Access Authentication" a "Basic Access Authentication".

5. Inserire nella casella di inserimento "Timeout RADIUS" il tempo in secondi che deve attendere al massimo l'unità Security per la risposta del server RADIUS.
6. Inserire nella casella di inserimento "Ripetizioni RADIUS" il numero di tentativi di collegamento con il server RADIUS.
7. Attivare la casella di controllo "Consenti autenticazione RADIUS di utenti non progettati", se al set di regole IP personalizzato da attivare è stato assegnato un ruolo anziché un utente.
8. Attivare la casella di controllo "L'ID filtro è necessario per l'autenticazione", se il ruolo assegnato è un ruolo personalizzato.
9. Fare clic sul pulsante "Aggiungi".

   Risultato: Il server RADIUS progettato per primo viene assegnato all'unità Security.

10. Selezionare eventualmente nella casella di riepilogo "Nome" il server RADIUS che si vuole assegnare all'unità Security.

Le informazioni generali relative all'autenticazione mediante server RADIUS si trova nel seguente capitolo:
Autenticazione mediante server RADIUS (Pagina 75)

Vedere anche

Crea utente (Pagina 66)

2.6 Gestione dei certificati

2.6.1 Informazioni generali

Come si gestiscono i certificati?

Nel manager dei certificati è riportato un sommario di tutti i certificati /certificati CA utilizzati nel progetto con indicazioni del richiedente, dell'emittente, della validità, dell'utilizzo in SCT e della presenza di una chiave privata.

Il certificato CA è un certificato emesso da un'autorità di certificazione, la cosiddetta "Certificate Authority", dalla quale vengono trasmessi i certificati dell'apparecchio. Dei certificati del dispositivo parte i certificati SSL necessari per l'autenticazione in caso di comunicazione online tra un'unità Security e un altro nodo di rete. Ulteriori certificati del dispositivo sono i certificati dei gruppi VPN di unità Security che si trovano nei gruppi VPN. Le autorità di certificazione possono essere:

- il SCT stesso. Se il "Richiedente" e l'"Emittente" sono uguali, si tratta di un certificato autofirmato emesso dal SCT.
- Un'autorità di certificazione sovraordinata. I certificati di terzi esterni al progetto vengono importati e salvati nella memoria dei certificati del SCT.

I certificati creati da una delle due autorità di certificazione dispongono sempre di una chiave privata con la quale i certificati degli apparecchi possono essere trasmessi.

Inoltre, nel manager dei certificati sono disponibili le seguenti funzioni per la selezione:

- Importazione di nuovi certificati e autorità di certificazione.
- Importazione di certificati FTPS se il CP viene utilizzato come client FTP. S7-CP
- Esportazione dei certificati e delle autorità di certificazione utilizzati nel progetto.
- Sostituzione di certificati scaduti e di autorità di certificazione.
- Sostituzione di autorità di certificazione esistenti.

Nota

Caricamento del progetto

Dopo la sostituzione o il rinnovo di certificati il progetto deve essere caricato nell'unità Security corrispondente.

Dopo la sostituzione o il rinnovo di certificati CA il progetto deve essere caricato in tutte le unità Security.

Nota

Data attuale e ora attuale sulle unità Security

In caso di utilizzo di comunicazione protetta (ad es. HTTPS, VPN...) fare attenzione che le unità Security interessate dispongano dell'ora e della data attuale. I certificati utilizzati vengono altrimenti valutati non validi e la comunicazione protetta non funziona.

A questa funzione si accede nel modo seguente

Voce di menu SCT: "Opzioni" > "Manager dei certificati...".

Nelle singole schede sono disponibili i seguenti pulsanti:

Pulsante	Descrizione
Importa... / Esporta...	Importazione / esportazione di certificati degli apparecchi o certificati CA non creati nell'SCT. I certificati vengono trasmessi all'unità Security. Sono consentiti i seguenti formati: *.pem (solo certificato) *.crt (solo certificato) *.p12 (certificati con relativa chiave privata) **Avvertenza** • Gli utenti con il ruolo definito dal sistema "diagnostics" non possono eseguire nessuna esportazione.
Visualizza....	Apre la finestra di dialogo dei certificati di Windows, nella quale viene visualizzato un sommario di tutti i dati dei certificati.

Scheda "Autorità di certificazione"

I certificati qui visualizzati vengono creati da un'autorità di certificazione.

- Autorità di certificazione di un progetto: Durante la creazione di un nuovo progetto SCT, per il progetto viene generato un certificato CA. Da questo certificato vengono trasmessi i certificati SSL per le singole unità Security.
- Autorità di certificazione di un gruppo VPN: Durante la creazione di un nuovo gruppo VPN, per il gruppo VPN viene generato un certificato CA. Per questo certificato vengono trasmessi i certificati dei gruppi VPN che si trovano nel gruppo VPN corrispondente.

Scheda "Certificato degli apparecchi"

Visualizzazione dei certificati specifici per il dispositivo generati dal SCT per un'unità Security. Ne fanno parte:

- Certificato SSL di un'unità Security: Per ciascuna unità Security creata viene generato un certificato SSL che deriva dal certificato CA del progetto. Per l'autenticazione i certificati SSL vengono inclusi nella comunicazione tra PG/PC e unità Security, nel caricamento della configurazione (non per CP) e nel logging.
- Certificato del gruppo SSL di un'unità Security: Inoltre per ciascuna unità Security per ogni gruppo VPN, nel quale si trova, viene generato un certificato del gruppo VPN.

Scheda "Certificati e autorità di certificazione accreditati"

Visualizzazione dei certificati di terzi importati nell'SCT. Possono essere importati ad es. certificati server da server FTP esterni o certificati di progetto di altri progetti SCT.

Il certificato di terzi importato viene trasmesso a tutti i CP gestiti nel progetto SCT. Con questo certificato l'unità Security può identificarsi durante l'accesso ad un server TPS. La progettazione SCT stessa non utilizza il certificato importato.

Visualizzazione delle autorità di certificazione necessarie per la verifica di servizi esterni quali i provider di DNS dyn. da parte di unità Security.

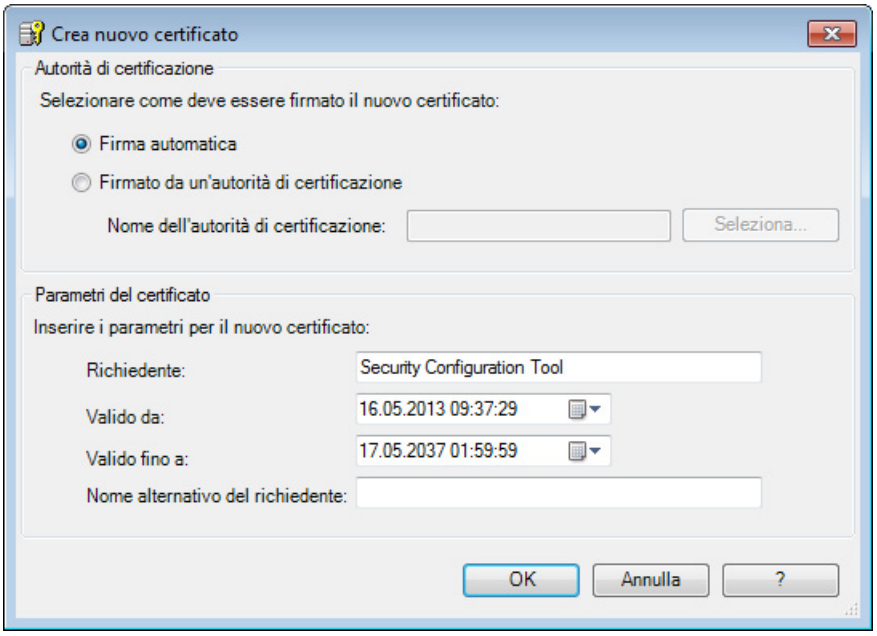
2.6.2 Rinnovo dei certificati

Significato

In questa finestra di dialogo si rinnovano i certificati CA e i certificati del dispositivo. In caso di necessità, ad es. con certificati compromessi, è possibile importare un certificato o generare un nuovo certificato dal Security Configuration Tool.

A questa funzione si accede nel modo seguente

1. Fare clic con il tasto destro del mouse su una voce dell'elenco nel manager dei certificati.
2. Selezionare la voce "Rinnova certificato ...".



3. Selezionare se il nuovo certificato deve essere autofirmato o se deve essere firmato da un'autorità di certificazione.
4. Se il certificato deve essere firmato da un'autorità di certificazione, selezionare con il pulsane "Seleziona..." l'autorità di certificazione da utilizzare. Per la selezione sono disponibili solo le autorità di certificazione memorizzate nella memoria dei certificati del progetto SCT attuale.
5. Selezionare un periodo nel quale il certificato è valido. Come standard nelle caselle "Valido da:" e "Valido fino a:" viene inserito il valore del certificato attuale.
6. A seconda del certificato inserire i seguenti valori:

Certificato da rinnovare	Parametri	
	Richiedente	Nome alternativo del richiedente
Certificato CA del progetto	Nome del certificato CA	-
Certificato CA del gruppo VPN	Nome del certificato CA	-
Certificato SSL per CP S7	Nome dell'unità Security	Indirizzi IP dell'interfaccia Gigabit e PROFINET, separati da una virgola.
Certificato SSL per CP PC	Nome dell'unità Security	Indirizzo IP dell'unità Security.
Certificato SSL per SCALANCE S, SCALANCE M e SOFTNET Security Client	Nome dell'unità Security	-
Certificato del gruppo SSL di un'unità Security	Nome del certificato del gruppo VPN	Trasmesso da CA.

2.6.3 Sostituzione di certificati

Significato

In questa finestra di dialogo si sostituisce un certificato CA esistente del progetto o il certificato CA di un gruppo VPN con uno nuovo.

A questa funzione si accede nel modo seguente

1. Fare clic con il tasto destro del mouse su una voce dell'elenco nella scheda "Autorità di certificazione".
2. Selezionare la voce "Sostituisci certificato...".
3. La finestra di dialogo "Sostituzione dell'autorità di certificazione" viene aperta.

Tutti i certificati elencati nella casella "Certificati interessati" vengono trasmessi di nuovo. In questo modo il certificato CA di un gruppo VPN già progettato all'interno del progetto SCT può essere sostituito con il certificato CA del gruppo VPN di un altro progetto SCT. I certificati del gruppo VPN per i nodi del gruppo VPN vengono quindi trasmessi in entrambi i progetti dallo stesso certificato CA.

Se durante la chiusura del manager dei certificati compare una finestra di dialogo di avvertenza, caricare di nuovo la configurazione modificata nell'unità Security.

Che formato può avere il certificato?

Dal certificato CA importato vengono trasmessi altri certificati in SCT. Per questo motivo possono essere selezionati solo certificati con chiave privata:

- *.p12

Creazione di unità e impostazione dei parametri di rete

3

Questo capitolo descrive come vengono create le unità e quali impostazioni sono possibili per le singole unità in un progetto.

Altre informazioni

Le informazioni dettagliate sulle finestre di dialogo e i parametri impostabili si trovano anche nella guida in linea.

Alla guida è possibile accedere con il tasto F1 o con il pulsante "Help" nella relativa finestra di dialogo SCT.

Nota

Potenzialità e tipi di apparecchio

Osservare le funzioni supportate dal tipo di apparecchio utilizzato.

Vedere anche

Funzioni online - Diagnostica e logging (Pagina 249)

A questa funzione si accede nel modo seguente

1. Selezionare l'oggetto "Tutte le unità" nell'area di navigazione.
2. Selezionare la voce di menu "Inserisci" > "Unità".
3. Eseguire le seguenti impostazioni.

Parametri	Significato
Tipo di prodotto	Tipo di prodotto che viene utilizzato durante la creazione di una nuova unità. SCALANCE S SCALANCE M Configurazione SOFTNET (SOFTNET Security Client, dispositivo VPN, client VPN NCP)
Unità	A seconda della selezione del tipo di prodotto è possibile indicare qui il tipo di unità che viene utilizzato durante la creazione di una nuova unità. Selezionare l'opzione "NCP client VPN per Android" per inserire il dispositivo client VPN, che sostituisce un dispositivo con software NCP Secure VPN Client for Android installato. Selezionare l'opzione "Dispositivo VPN" per inserire un dispositivo client VPN che sostituisce un dispositivo di un altro produttore. Avvertenza Il file di configurazione trasmesso rappresenta solo un supporto per la configurazione del collegamento VPN, ma non è una garanzia per una compatibilità con i prodotti di altri produttori.
Release del firmware	Per le unità SCALANCE S e per il SOFTNET Security Client possono essere indicati la versione firmware / e software. Osservazione: se si seleziona l'opzione "V4" per il SOFTNET Security Client si dispone dell'insieme completo delle funzioni di SOFTNET Security Client V4 e V5.
Nome dell'unità	Nome dell'unità a scelta.
Indirizzo MAC	Inserimenti dell'indirizzo MAC dell'unità
Indirizzo IP (est.)	Indirizzo IP per l'interfaccia esterna. L'indirizzo IP è composta da 4 numeri decimali dell'area di valori compresa tra 0 e 255, separati tra loro da un punto, ad es. 141.80.0.16
Maschera sotto-rete (est.)	Area dei valori per maschera della sotto-rete. Viene proposta in base all'indirizzo IP inserito. La maschera della sotto-rete è composta da 4 numeri decimali dell'area di valori compresa tra 0 e 255, separati tra loro da un punto, ad es. 255.255.0.0
Routing interfaccia esterno/interno	Selezione del modo di funzionamento per l'unità Security. Per SCALANCE S sono disponibili i seguenti modi di funzionamento: • modalità bridge • Modalità Routing Se si seleziona la modalità Routing è necessario progettare una maschera della sottorete per l'interfaccia interna dell'unità Security.
Indirizzo IP (int.) da inserire solo se è attivata la modalità routing	Indirizzo IP per l'interfaccia interna. L'indirizzo IP è composto da 4 numeri decimali dell'area di valori compresa tra 0 e 255, separati tra loro da un punto; ad es. 141.90.10.10

Parametri	Significato
Maschera sotto-rete (int.) da inserire solo se è attivata la modalità routing	Area dei valori per maschera della sotto-rete. La maschera della sotto-rete viene proposta in base all'indirizzo IP inserito. La maschera della sotto-rete è composta da 4 numeri decimali dell'area di valori compresa tra 0 e 255, separati tra loro da un punto, ad es. 255.255.0.0
Salvataggio della selezione	Se si attiva questa funzione la configurazione attualmente impostata viene acquisita nei valori di inizializzazione standard. Inserendo nuove unità viene più aperta la finestra di dialogo "Selezione di un'unità o di una configurazione software", ma viene inserita subito un'unità in base alle impostazioni definite nel progetto. Per disattivare di nuovo questa funzione e selezionare un altro tipo di unità, questa funzione deve essere disattivata dal seguente percorso di menu: "Progetto" > "Proprietà..." > "Valori di inizializzazione standard"

Nota

Impostazioni supplementari

Eseguire ulteriori impostazioni dell'interfaccia nella scheda "Interfacce" delle proprietà dell'interfaccia. Informazioni su questo argomento si trovano nel capitolo:

- Configurazione delle interfacce (Pagina 90)

Creazione di CP in STEP 7

I CP vengono creati solo in STEP 7. Essi compaiono dopo la creazione e la definizione come unità Security nelle proprietà dell'unità di STEP 7, nell'elenco delle unità configurate nell'SCT. I dati dell'indirizzo vengono acquisiti da STEP 7 e non possono essere modificati nell'SCT.

Vedere anche

Parametri nell'area del contenuto (Pagina 88)

Aree dei valori indirizzo IP, maschera della sottorete indirizzo dell'accoppiamento ad altra rete (Pagina 263)

MAC adress (Pagina 264)

3.1 Parametri nell'area del contenuto

Alla visualizzazione si accede nel modo seguente

Selezionare l'oggetto "Tutte le unità" nell'area di navigazione.

Per i CP possono essere modificati solo i contenuti della colonna "Commento".

Le seguenti proprietà delle unità vengono visualizzate per colonne:

Proprietà/colonna	Significato	Commento/selezione
N.	Numero progressivo di unità	viene assegnato automaticamente
Name	Denominazioni univoca dell'unità	selezionabile liberamente
Typ	Tipo di apparecchio	**Avvertenza** Per i dispositivi del tipo "SOFTNET Security Client" e "NCP client VPN per Android" non esiste nessuna finestra di dialogo delle proprietà. Per i dispositivi VPN, nelle proprietà dell'unità è possibile adattare solo i tipi di file dei file di configurazione da esportare.
Ext. IP address	Indirizzo IP con il quale è raggiungibile il dispositivo nella rete esterna, ad es. per caricare la configurazione	assegnazione adatta nell'insieme di reti.
Maschera sotto-rete est.	Maschera della sottorete per l'indirizzo IP esterno	assegnazione adatta nell'insieme di reti.
Int. IP address	Indirizzo IP con il quale è raggiungibile il dispositivo della rete interna, se configurato come router	assegnazione adatta nell'insieme di reti. La casella di inserimento può essere editata solo se la modalità routing è attivata.
Maschera sotto-rete int.	Maschera della sottorete per l'indirizzo IP interno	assegnazione adatta nell'insieme di reti. La casella di inserimento può essere editata solo se la modalità routing è attivata.
Router standard	Indirizzo IP del router standard	assegnazione adatta nell'insieme di reti.
MAC address	Indirizzo hardware dell'unità	L'indirizzo MAC è stampigliato sulla custodia dell'unità.
Comment	Informazioni sull'unità e sulla sotto-rete protetta dall'unità	selezionabile liberamente

Modifica dei parametri di indirizzo per SCALANCE S / M

Per le unità SCALANCE S / M alcuni parametri di indirizzo possono essere inseriti e modificati nell'area del contenuto.

Significato dei parametri di indirizzo per CP

CP

Per i CP vengono visualizzati i seguenti indirizzi da STEP 7:

Casella nell'SCT	CP x43-1 Adv.	CP 1628
Indirizzo IP est	Indirizzo IP Gigabit	Indirizzo IP IE (Industrial Ethernet)
Maschera sotto-rete est.	Maschera della sotto-rete Gigabit	Maschera della sotto-rete IE
Indirizzo IP Int.	Indirizzo IP PROFINET	Non viene visualizzato
Maschera sotto-rete int.	Maschera della sotto-rete PROFINET	Non viene visualizzato
Router standard	Router standard progettato in STEP 7	Router standard progettato in STEP 7
Indirizzo MAC	Indirizzo MAC Gigabit (se progettato)	Indirizzo MAC IE (se progettato)

Vengono visualizzati anche i dati di indirizzo nella scheda "Interfacce".

indirizzo IP assegnato dinamicamente

S7-CP

Se in STEP 7 è progettato che l'indirizzo IP deve essere assegnato dinamicamente, esso viene rappresentato nell'SCT in base alle impostazioni nel modo seguente:

Tabella 3- 1 Interfaccia gigabit

Moto di funzionamento in STEP 7	Indirizzo IP est. / maschera della sotto-rete est. (caselle in SCT)
Rilevamento dell'indirizzo IP da un DHCP Server	dinamico

Tabella 3- 2 Interfaccia PROFINET

Moto di funzionamento in STEP 7	Indirizzo IP int. / maschera della sotto-rete int. (caselle in SCT)
Rilevamento dell'indirizzo IP da un DHCP Server	dinamico
Impostazione dell'indirizzo IP nel programma utente	
Impostazione dell'indirizzo IP su un altro percorso	

3.2 Configurazione delle interfacce

3.2.1 Panoramica delle possibilità di collegamento

SCA. S

Possibilità di collegamento supportate

Ciascuna unità Security dispone di un determinato numero di porte alle quali possono essere collegati i nodi di rete. In base alla rispettiva interfaccia, i nodi di rete vengono trattati in modo diverso.

Unità Security	Interfaccia	Indirizzo MAC dell'interfaccia*	Porta dell'interfaccia	Tipo di porta	Indirizzo MAC della porta*
SCALANCE S602 / S612 / S613	Esterno	Indirizzo MAC (vedere stampigliatura)	P1	Presa RJ-45 montata in modo fissa (rame)	Indirizzo MAC + 2
	Interno	Indirizzo MAC + 1	P2	Presa RJ-45 montata in modo fissa (rame)	Indirizzo MAC + 3
SCALANCE S623	Esterno	Indirizzo MAC (vedere stampigliatura)	P1	Presa RJ-45 montata in modo fissa (rame)	Indirizzo MAC + 3
	Interno	Indirizzo MAC + 1	P2	Presa RJ-45 montata in modo fissa (rame)	Indirizzo MAC + 4
	DMZ	Indirizzo MAC + 2	P3	Presa RJ-45 montata in modo fissa (rame)	Indirizzo MAC + 5
SCALANCE S627-2M	Esterno	Indirizzo MAC (vedere stampigliatura)	P1	Presa RJ-45 montata in modo fissa (rame)	Indirizzo MAC + 3
			P4	Porta modulo mediale (rame/FO)	Indirizzo MAC + 4
			P5	Porta modulo mediale (rame/FO)	Indirizzo MAC + 5
	Interno	Indirizzo MAC + 1	P2	Presa RJ-45 montata in modo fissa (rame)	Indirizzo MAC + 6
			P6	Porta modulo mediale (rame/FO)	Indirizzo MAC + 7
			P7	Porta modulo mediale (rame/FO)	Indirizzo MAC + 8
	DMZ	Indirizzo MAC + 2	P3	Presa RJ-45 montata in modo fissa (rame)	Indirizzo MAC + 9

* In caso di funzionamento in modalità Bridge, sull'interfaccia esterna ed interna è sempre valido l'indirizzo MAC stampigliato.

Gli indirizzi MAC delle interfacce vengono utilizzate per tutti i servizi tranne LLDP.

Gli indirizzi MAC delle porte vengono utilizzate per il riconoscimento della topologia con LLDP (solo per unità in modalità Routing).

Nota

Le interfacce Ethernet non devono essere scambiate durante il collegamento alla rete di comunicazione:

- Interfaccia X1 - esterna
  Contrassegno rosso = area di rete non protetta;
- Interfaccia X2 - interna
  Contrassegno verde = rete protetta con SCALANCE S;
- Interfaccia X3 - DMZ (interfaccia di rete universale)
  Contrassegno giallo = area di rete non protetta o area di rete protetta con SCALANCE S.

In caso di scambio delle interfacce il dispositivo perde la sua funzione di protezione.

Funzioni delle interfacce DMZ S62x

Una zona demilitarizzata (DMZ) viene utilizzata se devono essere forniti servizi per una rete esterna e la rete interna, che fornisce dati per questi servizi, deve essere disaccoppiata dalla rete esterna. Nella DMZ possono trovarsi ad es. server terminal, sui quali sono installati programma di manutenzione e di diagnostica che consentono accessi definiti a determinati sistemi nella rete protetta. Hanno accesso solo utenti o client autorizzati dalla rete non protetta o client collegati tramite VPN. Le regole firewall possono essere progettate in modo che da Internet siano possibili accessi a dispositivi nella DMZ, ma non alla rete interna. Per una maggiore protezione è possibile limitare gli accessi consentiti esclusivamente al traffico di dati via VPN. Una configurazione generica, nella quale l'interfaccia DMZ viene utilizzata per la configurazione di una DMZ, viene eseguita e documentata nel capitolo "4.2 SCALANCE S come firewall tra rete esterna e DMZ" del manuale "SIMATIC NET Industrial Ethernet Security - Configurazione di Security".
Per poter assegnare anche ai dispositivi nella DMZ un indirizzo IP dinamico, sull'interfaccia DMZ può essere attivato un server DHCP. Tuttavia in un caso applicativo di questo tipo è necessario assicurarsi che gli apparecchi nel DMZ ricevano sempre lo stesso indirizzo IP via DHCP, in quanto questi indirizzi IP vanno utilizzati per la configurazione firewall. Ciò significa che durante la progettazione DHCP non deve essere utilizzata l'assegnazione dinamica dell'indirizzo, ma solo l'assegnazione statica dell'indirizzo in base all'indirizzo MAC o alla ID client.

L'interfaccia DMZ può essere utilizzata come punto terminale VPN. In combinazione con un modem DSL l'interfaccia DMZ viene utilizzata in modalità PPPoE o, in combinazione con un router DSL inserito a monte, con l'indirizzo IP statico. Una configurazione generica, nella quale l'interfaccia DMZ viene utilizzata come accesso remoto tramite un tunnel VPN, viene eseguita nel capitolo "5.2 Tunnel VPN tra SCALANCE S623 e SCALANCE S612" del manuale "SIMATIC NET Industrial Ethernet Security - Configurazione di Security".

Porte del modulo mediale dell'interfaccia esterna e interna S627-2M

Oltre alle funzioni di SCALANCE S623, SCALANCE S627-2M dispone di due slot modulo mediale nei quali può essere inserito rispettivamente un modulo mediale elettrico o ottico a 2 porte. In questo modo l'interfaccia esterna ed interna può essere ampliata rispettivamente di due porte. Se per un'interfaccia viene utilizzato il modulo mediale "MM992-2SFP", nel modulo mediale di questa interfaccia è possibile inserire fino a due transceiver SFP elettrici o ottici (Small Form-factor Pluggable Transceiver). Le porte supplementari possono essere utilizzate per il collegamento dell'interfaccia esterna ed interna di SCALANCE S627-2M ad anelli MRP/HRP.

Le porte del modulo mediale sono collegate alle porte fisse della relativa interfaccia tramite un blocco switch. Tra le porte collegate tramite un blocco switch non è garantita la funzionalità firewall (livello 2 / livello 3). Tutte le porte collegate tramite un blocco switch sono raggiungibili tramite lo stesso indirizzi IP.

Funzioni delle singole interfacce

Le seguenti funzioni possono essere utilizzate sulle singole interfacce:

Funzionamento	Verde (interna)	Rossa (esterna)	Gialla (DMZ)
Indirizzo IP statico	x	x	x
Accesso WAN con router DSL	-	x	x
Accesso WAN con modem DSL (PPPoE, indirizzo IP dinamico di ISP)	-	x (In caso contrario sull'interfaccia gialla)	x (In caso contrario sull'interfaccia rossa)
modalità bridge	x		-
Modalità Routing	x	x	x
Modalità Ghost S602 ≥V3.1	-	x	-
Server DHCP	x	-	x
Punto terminale di un collegamento via tunnel VPN (con modem DSL e router DSL)	-	x	x
Client MRP/HRP (in modalità routing, porte dell'anello sui moduli mediali) S627-2M	x	x	-
LLDP (in modalità Routing) S≥V4.0	x	x	x

Funzionamento	Verde (interna)	Rossa (esterna)	Gialla (DMZ)
Listening passivo (in modalità Routing se sono inseriti moduli mediali) S627-2M	x	x	-

x è supportato

- non è supportato

Metodo Duplex

Per una porta può essere selezionato uno dei due metodi Duplex:

- Halfduplex: L'unità Security può o ricevere o inviare dati.
- Fullduplex: L'unità Security può o ricevere e inviare dati simultaneamente.

Nota

Metodo duplex e velocità di trasmissione con porte ottiche S627-2M

Per le porte con il tipo di porta "Ottica" la modalità della porta è definita in modo fisso dal modulo mediale utilizzato o dall'SFP utilizzato e non può essere adattata.

3.2.2 Interfacce

SCA. S

SCA. M

A questa funzione si accede nel modo seguente:

1. Selezionare l'unità da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "Interfacce"

Routing interfaccia - Possibilità di selezione SCA. S

Se l'unità SCALANCE S non si trova in nessun gruppo VPN e in nessuna relazione di ridondanza, il routing dell'interfaccia in questa casella può essere modificato. La selezione vale per il routing tra l'interfaccia esterna e l'interfaccia interna. L'interfaccia DMZ (solo SCALANCE S623 und SCALANCE S627-2M) viene sempre collegata in modalità Routing.

modalità bridge	Per il funzionamento nelle reti piatte. L'interfaccia esterna e l'interfaccia interna si trovano nella stessa sotto-rete IP. Per S623 / S627-2M: L'interfaccia esterna e quella interna si trovano nella stessa sottorete IP, l'interfaccia DMZ si trova in un'altra sottorete IP o è in modalità di funzionamento o è disattivata.
Modalità Routing	Tutte le interfacce si trovano in diverse sotto-reti IP. **Avvertenza** Se per l'unità SCALANCE S è stata attivata la modalità routing, non possono essere definite le regole MAC.
Modalità Ghost S602 ≥V3.1	Durante il funzionamento l'unità SCALANCE S acquisisce per l'interfaccia interna l'indirizzo IP del nodo collegato all'interfaccia interna dell'unità SCALANCE S. I dati di indirizzo IP da indicare per l'interfaccia esterna servono solo per il caricamento della progettazione prima del funzionamento in modalità Ghost. **Avvertenza** Nella scheda "Interfacce" la modalità Ghost può essere selezionata solo se il progetto si trova in modalità estesa.

Progettazione delle interfacce

Se deve essere progettata l'interfaccia di un'unità, essa deve essere attivata tramite la casella di controllo "Attiva interfaccia". Definire le indicazioni di indirizzo IP per ciascuna interfaccia e le impostazioni delle singole porte (solo per SCALANCE S a partire da V3). Per l'assegnazione di un indirizzo IP, per l'interfaccia esterna e per l'interfaccia DMZ (solo SCALANCE S623/S627-2M) sono disponibili le seguenti modalità di assegnazione:

- Indirizzo IP statico con maschera della sotto-rete
- Assegnazione di indirizzi tramite PPPoE S≥V3.0

  L'interfaccia interna e l'interfaccia tunnel (solo per SCALANCE S612/S623/S627-2M a partire da V4) possono essere progettate solo tramite un indirizzo IP fisso.

Se mediante progettazione di una regola NAT/NAPT per un'unità SCALANCE S sono stati registrati indirizzi IP Alias su un'interfaccia, essi vengono visualizzati nella casella "Indirizzi IP Alias".

Nota

Interfaccia esterna e interfaccia DMZ (solo SCALANCE S623/S627-2M) come accesso a Internet

Non è possibile il funzionamento simultaneo di PPPoE sull'interfaccia esterna e sull'interfaccia DMZ (ISP duale).

Significato dell'indirizzo IP tunnel S≥V4.0 ~~S602~~

Se si utilizza la funzione "NAT/NAPT con tunnel VPN" è necessario assegnare un indirizzo IP tunnel per l'unità Security. In questo modo viene assicurata la raggiungibilità dell'unità Security tramite il tunnel VPN e garantita una possibilità di configurazione e di diagnostica. All'indirizzo IP tunnel progettato possono essere aggiunti indirizzi IP tunnel Alias utilizzando regole NAT/NAPT corrispondenti. La maschera della sottorete è definita in modo fisso a 32 bit per l'indirizzo IP tunnel e non può essere modificato. L'indirizzo IP tunnel può essere progettato solo se vengono soddisfatti i seguenti requisiti:

- L'unità Security si trova in un gruppo VPN.
- Il progetto si trova in modalità estesa.

Ulteriori informazioni sulla conversione di indirizzi con NAT/NAPT in tunnel VPN si trovano nel seguente capitolo:
Conversione di indirizzi con tunnel NAT/NAPT nei tunnel VPN (Pagina 174)

Point to Point Protocol over Ethernet (PPPoE) S≥V3.0

Per consentire una connessione a Internet/WAN direttamente tramite un modem DSL, l'assegnazione dell'indirizzo IP sull'interfaccia esterna o sull'interfaccia DMZ avviene tramite PPPoE. PPPoE è un protocollo di accesso remoto per rilevare indirizzi IP da un Internet Service Provider (ISP). SCALANCE S in quindi utilizzato in modalità routing

Per utilizzare questo metodo di assegnazione di indirizzi IP inserire le indicazioni relative a ISP nella scheda "Collegamento Internet". L'indirizzo IP, la maschera della sottorete, il router standard e il server DNS dell'interfaccia vengono predefiniti dall'ISP.

Nota

Un router standard progettato non viene tenuto in considerazione in caso di utilizzo di PPPoE. Esso viene assegnato dinamicamente all'unità dall'ISP.

Nota

Nessun componente di rete tra SCALANCE S e modem DSL

Se l'interfaccia di un'unità SCALANCE S viene utilizzata tramite PPPoE, tra questa interfaccia e il modem DSL collegato non devono trovarsi altri componenti di rete in quanto i dati di selezione dell'Internet Service Provider vengono event. trasmessi senza codifica su questo percorso. In caso di utilizzo del protocollo di autenticazione "CHAP" i dati possono essere trasmessi senza codifica.

Impostazioni porta S≥V3.0

Colonna	Significato		
ID porta	ID indicata automaticamente per la porta dell'interfaccia.		
Tipo di porta	Proprietà finisca della porta (rame/FO)		
Modalità porta	Autonegotiation	La velocità di trasmissione e il metodo duplex vengono gestiti automaticamente tra porte conformi a IEEE 802.3. **Avvertenza** Una velocità di trasmissione di 1000 MBit/s e la funzione Autocrossing vengono supportate solo se l'Autonegotiation è selezionata.	
	10 MBit/s, halfduplex e fullduplex	Velocità di trasmissione di 10 Mbit/s	
	100 MBit/s, halfduplex e fullduplex	Velocità di trasmissione di 100 Mbit/s	
	Long Distane Segnalino (LDS)	La velocità di trasmissione e il metodo duplex vengono gestiti automaticamente tra porte conformi a Broda-Reach.	
	Off (solo porta esterna o porta DMZ con SCALANCE S623 e SCALANCE S627-2M)	La porta viene disattivata.	
	Avvertenza S627-2M Le porte dei moduli mediali che come mezzo trasmissivo utilizzano cavi a fibre ottiche funzionano già con il metodo fullduplex e la velocità di trasmissione massima. La modalità delle porte di moduli mediali ottici non può quindi essere progettata.		
S≥V4.0 Modalità LLDP (in modalità Routing)	RxTx	Invio e ricezione di telegrammi LLDP	Maggiori informazioni relative a LLDP si trovano nel seguente capitolo: LLDP (Pagina 101)
	Off	Ricezione di telegrammi LLDP	

Colonna	Significato
S627-2M Porta MRP (in modalità Routing per le porte del modulo mediale dell'interfaccia esterna ed interna)	Indicazione se le porte del modulo mediale dell'interfaccia sono collegate ad un anello MRP. In questo caso le stringhe di caratteri "RingportOne" e "RingportTwo" vengono visualizzate nelle righe della tabella delle porte del modulo mediale. Per le porte con IP porta "X1 P1" e "X2 P1" come standard viene visualizzata la stringa di caratteri "None" in quando esse non possono essere coinvolte in un anello MRP. Informazioni generali sulla ridondanza del mezzo con MRP si trovano nel seguente capitolo: Ridondanza del mezzo con MRP/HRP (Pagina 102) Informazioni sulla progettazione di MRP per unità Security si trovano nel seguente capitolo: Progettazione MRP/HRP per le unità Security (Pagina 103)
S627-2M Porta HRP (in modalità Routing per le porte del modulo mediale dell'interfaccia esterna ed interna)	Indicazione se le porte del modulo mediale dell'interfaccia sono collegate ad un anello HRP. In questo caso le stringhe di caratteri "RingportOne" e "RingportTwo" vengono visualizzate nelle righe della tabella delle porte del modulo mediale. Per le porte con IP porta "X1 P1" e "X2 P1" come standard viene visualizzata la stringa di caratteri "None" in quando esse non possono essere coinvolte in un anello HRP. Informazioni generali sulla ridondanza del mezzo con HRP si trovano nel seguente capitolo: Ridondanza del mezzo con MRP/HRP (Pagina 102) Informazioni sulla progettazione di HRP per unità Security si trovano nel seguente capitolo: Progettazione MRP/HRP per le unità Security (Pagina 103)
Commento	Commento liberamente selezionabile

Configurazione dei moduli mediali S627-2M

Fare clic sul pulsante "Configura modulo mediale..." per richiamare la finestra di dialogo per la configurazione del modulo mediale per l'interfaccia corrispondente.

Per la selezione sono disponibili le seguenti modalità di configurazione:

- "Automatico" (impostazione standard): Il modulo mediale utilizzato viene riconosciuto automaticamente durante il funzionamento. La modalità della porta viene impostata per entrambe le porti su "Auto-Negotiation".
- "Manuale": Selezionare il tipo di modulo mediale utilizzato dalla casella di riepilogo "Tipo di modulo". Se si seleziona il tipo di modulo mediale "MM992-2SFP", dalle due caselle di riepilogo "Tipo SFP" è possibile selezionare i transceiver ad innesto (SFP) desiderati. Per le porte con il tipo di porta "Rame" è possibile definire manualmente la velocità di trasmissione nonché il metodo duplex tramite la modalità della porta. Per le porte con il tipo di porta "Ottica" la modalità della porta è definita in modo fisso dal modulo mediale utilizzato o dall'SFP utilizzato e non può essere adattata.

Vedere anche

Particolarità della modalità Ghost (Pagina 105)

Panoramica delle possibilità di collegamento (Pagina 90)

Dati di configurazione per le unità SCALANCE M (Pagina 210)

3.2.3 Collegamento Internet

S≥V3.0

A questa funzione si accede nel modo seguente:

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "Collegamento Internet"

Significato

Se per un'interfacce dell'unità Security è impostato un collegamento tramite PPPoE, eseguire in questa scheda le impostazioni per l'Internet Service Provider (ISP).

Tabella 3- 3 Impostazioni per l'account ISP

Funzionamento	Descrizione
Nome utente	Inserire il nome per il login nell'account ISP.
Password	Inserire la password per il login nell'account ISP.
Conferma password	Inserire di nuovo la password per il login nell'account ISP.
Autenticazione	Non selezionare nessun protocollo di autenticazione o selezionarne uno dei seguenti: • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) **Avvertenza** Entrambi i partner di comunicazione devono utilizzare lo stesso metodo di autenticazione altrimenti non viene realizzato nessun collegamento.

Tabella 3- 4 Regole per nome utente e password

Caratteri ammessi	Sono consentiti i seguenti caratteri del set di caratteri ANSI X 3.4-1986: 0123456789 A...Z a...z !#$%&()"*'+`,-./:;<=>?@ [\]_{|}~^
Lunghezza del nome utente	1 ... 255 caratteri
Lunghezza della password	1 ... 31 caratteri

Tabella 3- 5 Impostazioni per il collegamento

Funzionamento	Descrizione
Collegamento duraturo	Collegamento Internet permanente. Dopo un'interruzione da parte del provider il collegamento viene ripristinato automaticamente anche se attualmente non devono essere inviati pacchetti.

Collegamento On-Demand	Il collegamento Internet viene realizzato automaticamente se i pacchetti devono essere inviati in Internet. In questa impostazione non sono possibili ritardi durante l'invio di pacchetti.
Disconnessione forzata (solo con l'impostazione "Collegamento permanente")	Il provider interrompe il collegamento internet dopo un determinato periodo. Se nella casella "Interruzione forzata" si inserisce un'ora, l'unità Security interrompe autonomamente a quest'ora il collegamento Internet. In questo modo è possibile eventualmente spostare una disconnessione del collegamento dal lato del provider. Una disconnessione autoinizializzata è possibile solo in caso di esistenza un collegamento permanente. Inserimenti consentiti: 00:00 ... 23:59
Tempo massimo di inattività (solo con l'impostazione "Collegamento On Demand")	Se entro un determinato periodo non vengono inviati pacchetti, il collegamento Internet viene interrotto automaticamente. Inserire nella casella "Tempo massimo di inattività" il tempo in secondi dopo il quale il collegamento deve essere interrotto. Valori consentiti: 10 … 3600.

Progettazione della conversione dell'indirizzo nella rete PPPoE

La casella di controllo "Consenti NAT dall'interno alla rete PPPoE" è disponibile solo se il progetto non si trova in modalità estesa. Se si attiva la casella di controllo, tramite SCT viene creata una regola NAT con la quale gli indirizzi IP sorgente di tutti i nodi nella rete interna vengono convertiti in indirizzo IP dell'unità nella rete PPPoE. Questa regola NAT nonché la relativa regola firewall è visibile dopo l'attivazione della casella di controllo in modalità estesa.

3.2.4 DNS dinamico (DDNS)

S≥V3.0

Significato

Con il DNS dinamico è possibile accedere ad un indirizzi IP che cambia continuamente con un nome definito in modo fisso (FQDN). Questo è necessario se ad es. si vuole accedere ad un server raggiungibile tramite un indirizzo IP pubblico variabile.

Tipo di funzione

L'unità Security segnala ad un provider per il DNS dinamico (ad es DynDNS.org, no-ip.com) l'indirizzo IP WAN attuale con il quale è raggiungibile l'unità Security. Il provider garantisce che alle richieste DNS sull'FQDN dell'unità Security pervenga l'indirizzo IP WAN attuale dell'unità Security come risposta.

Il DNS dinamico è ammesso sulle seguenti interfacce:

- Interfaccia esterna
- Interfaccia DMZ

Configurazione del DNS dinamico - requisito richiesto

Requisito richiesto:

- In uno provider per il DNS dinamico è creato un account ed è registrato un FQDN.

Configurazione del DNS dinamico - Procedimento:

1. Selezionare nelle proprietà dell'unità Security la scheda "DNS".
2. Se l'unità Security si trova a valle di un router DSL o di un modem DSL, inserire l'indirizzo di un server DNS valido. Per questa operazioni sono disponibili due opzioni:

Option	Significato
Rilevamento automatico dell'indirizzo server DNS	L'indirizzo del server DNS può essere rilevato automaticamente tramite PPPoE, se l'unità Security è collegata ad Internet tramite un modulo DSL. Può essere impostato solo per l'interfaccia esterna e l'interfaccia DMZ.
Utilizzare il seguente indirizzo server DNS:	Inserire manualmente l'indirizzo del server DNS preferito e di quello alternativo.

3. Attivare la casella di controllo "Attiva servizio" nell'area "Servizio DNS din. primario" ed eseguire le seguenti impostazioni:

Impostazione	Significato
Provider	Selezionare in quale provider è stato configurato un account DNS dinamico.
Account utente nel provider	Inserire il nome utente definito durante la creazione dell'account.
Password nel provider	Inserire la password definita durante la creazione dell'account.
FQDN	Inserire il nome host (ad es. mysecuritydevice) e il nome di dominio (ad es. dyndns.org) registrato dal provider, separato da un punto. Se anche nella scheda "VPN" è inserito un FQDN, entrambi devono corrispondere.
Sorveglianza del cambio di indirizzo IP sul router DSL	Se l'unità Security è collegata ad Internet tramite un router DSL, attivando la funzione viene attivato il servizio IP di controllo. L'unità Security invia periodicamente richieste per determinare l'indirizzo IP attuale del router DSL e per rilevare un cambio di indirizzo IP sul router DSL. L'indirizzo IP così determinato viene inviato al provider ad ogni riconoscimento di modifica.
Periodo	Inserire il ciclo nel quale viene richiamato il servizio IP di controllo. Valori consentiti: 10 … 1440 minuti

4. Creare un provider alternativo nel caso non funzionasse il provider primario nella scheda "Servizio DNS din. secondario" (impostazione opzionale).

Configurazione del provider personalizzato - Procedimento:

Selezionare dalla casella di riepilogo "Provider" la voce "Personalizzato" ed eseguire inoltre i seguenti inserimenti:

Impostazione	Significato
URL aggiornamento provider	Inserire il rispettivo URL ricevuto dal proprio provider. I testi segnaposto <FQDN> e <CurrentWanIP> devono quindi essere posizionati nella relativa posizione dell'URL.
URL servizio IP di controllo	Inserire il rispettivo URL ricevuto dal proprio provider.
Ignora errori durante il controllo del certificato del server	Per far sì che di dati di autenticazione siano protetti, come standard il certificato del server update è controllato. Se il controllo del certificato fallisce, il collegamento HTTPS viene chiuso e i dati dell'account non vengono trasmessi. Se si attiva la casella di controllo, la funzione viene disattivata, ad es. se il certificato del server del servizio DNS din. non è valido (ad es. è scaduto). Si raccomanda di non ignorare il controllo e di non attivare la casella di controllo.

3.2.5 LLDP

S≥V4.0

Significato

LLDP (Link Layer Discovery Protocol) è un protocollo che viene utilizzato per il riconoscimento delle topologie di rete. Un dispositivo con funzione LLDP è quindi in grado di inviare ad intervalli regolari informazioni sul proprio stato ai dispositivi adiacenti e di riceve simultaneamente informazioni dai dispositivi adiacenti. Le informazioni ricevute vengono salvate su ciascun dispositivo con funzione LLDP in un file MIB LLDP. I sistemi di gestione della rete possono accedere a questi file MIB LLDP mediante SNMP e quindi di formare successivamente la presente topologia di rete.

Parametri progettabili

L'entità di attività dell'unità Security in merito a LLDP può essere progettata nella scheda "Interfacce" delle proprietà dell'unità nel modo seguente:

- Invio e ricezione di telegrammi LLDP (impostazione standard, "RxTx")
- Ricezione di telegrammi LLDP ("Off")

3.2.6 Ridondanza del mezzo nelle topologie ad anello

3.2.6.1 Ridondanza del mezzo con MRP/HRP

S627-2M

Significato

Nel termine "Ridondanza del mezzi" vengono raggruppati diversi metodi per aumentare la disponibilità di reti Industrial Ethernet nelle quali i dispositivi sono raggiungibili tramite diversi percorsi. Questo può avvenire tramite interconnessione di reti, collegamento in parallelo di percorsi di trasmissione o chiusura di una topologia lineare in un anello.

Metodi di ridondanza del mezzo MRP e HRP

La ridondanza del mezzo all'interno di una topologia ad anello è disponibile per i prodotti SIMATIC NET nel metodo MRP (Media Redundancy Protocol) e HRP (High Speed Redundancy Protocol).

In entrambi i metodi uno dei nodi viene configurato come manager di ridondanza. Gli altri nodi sono client di ridondanza. Le unità SCALANCE S627-2M possono assumere solo il ruolo di un client MRP o HRP. Con i telegrammi di test il manager di ridondanza controlla che l'anello non presenti interruzioni. I client di ridondanza inoltrano i telegrammi di test. Se in caso di interruzione dell'anello i telegrammi di test del manager di ridondanza non pervengono più sull'altra porta dell'anello, il manager di ridondanza attiva entrambe le sue porte e informa i client della ridondanza del cambio.

Entrambi i metodi di ridondanza del mezzo MRP e HRP funzionano in base allo stesso principio di funzionamento. Essi si differenziano per la durata necessaria agli switch SCALANCE X come manager di ridondanza per attivare le porte dell'anello:

- MRP: 200 ms
- HRP: 300 ms

Avvertenza sull'impiego di MRP e HRP

- MRP e HRP viene supportato in topologie ad anello con fino a 100 dispositivi. Un superamento del numero di dispositivi può comportare l'interruzione del traffico di dati.
- Si raccomanda di impostare le porte dell'anello interessate su fullduplex e 100 Mbit/s. In caso contrario può verificarsi l'interruzione del traffico di dati.

Possibilità di impiego di MRP/HRP sulle porte del modulo mediale

MRP/HRP viene supportato solo sulle porte del modulo mediale di SCALANCE S627-2M. La seguente tabella indica le possibilità di impiego di MRP/HRP sulle porte del modulo mediale di uno SCALANCE S627-2M:

Porte dell'anello	Modulo mediale 1		Modulo mediale 2	
	P4	P5	P6	P7
Client MRP o client HRP*	-	-	-	-
	Anello 1	Anello 1	-	-
	-	-	Anello 2	Anello 2
	Anello 1	Anello 1	Anello 2	Anello 2

* Il collegamento simultaneo dell'unità Security ad un anello interno e un anello interno è possibile solo se almeno una delle interfacce viene collegata come client MRP.

In caso di due anelli subordinati per ciascuna unità SCALANCE S è possibile una comunicazione livello 3 tra gli anelli.

3.2.6.2 Progettazione MRP/HRP per le unità Security

S627-2M

Presupposti

- L'unità Security si trova in modalità Routing.
- Per le interfacce che devono essere collegate agli anelli sono progettati diversi moduli mediali.

A questa funzione si accede nel modo seguente

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "MRP/HRP"

Parametri configurabili

Parametri	Significato	Possibilità di selezione
Interfacce MRP/HRP	Selezione dell'interfaccia che deve essere collegata all'anello MRP/HRP.	• Esterno • Interno
Ruolo di ridondanza del mezzo	Selezione del protocollo di ridondanza del mezzo o disattivazione della ridondanza del mezzo per l'interfaccia selezionata.	• Non nodo dell'anello • Client MRP (impostazione standard) • HRP Client

Parametri	Significato	Possibilità di selezione
Attiva 'listening passivo'	Attivare questa casella di controllo se l'interfaccia selezionata deve essere accoppiata ad altre reti nelle quali viene utilizzato STP/RSTP (Spanning-Tree-Protocol/Rapid-Spanning-Tree-Protocol).	• Attiva "listening passivo" (impostazione standard) • Disattiva "listening passivo"
Dominio MRP (solo in caso di selezione del ruolo di ridondanza del mezzo "Client MRP")	Con i domini MRP vengono definiti i nodi di un anello MRP. Per le interfacce di tutte le unità che devono essere collegate allo stesso anello MRP è necessario selezionare lo stesso dominio MRP.	Come standard per l'interfaccia esterna è selezionato il dominio MRP predefinito "mrpdomain-1". Tramite i pulsanti "Aggiungi...", "Modifica..." e "Rimuovi" è possibile aggiungere nuovi domini MRP, modificare i nomi di domini MRP esistenti e cancellare domini MRP esistenti.
Porta anello 1 (solo in caso di selezione del ruolo di ridondanza del mezzo "Client MRP" o "Client HRP")	Denominazione della prima porta dell'anello dell'interfaccia selezionata in "Interfaccia" se per essa è stato selezionato il ruolo di ridondanza del mezzo "Client MRP" o "Client HRP".	-
Porta anello 2 (solo in caso di selezione del ruolo di ridondanza del mezzo "Client MRP" o "Client HRP")	Denominazione della seconda porta dell'anello dell'interfaccia selezionata in "Interfaccia" se per essa è stato selezionato il ruolo di ridondanza del mezzo "Client MRP" o "Client HRP".	-
Nodo MRP (solo in caso di selezione del ruolo di ridondanza del mezzo "Client MRP")	Indicazione delle informazioni su tutte le unità Security che fanno parte dello stesso dominio MRP dell'interfaccia selezionata.	-

Risultato

L'interfaccia Security è stata collegata all'anello MRP/HRP tramite l'interfaccia selezionata. Le porte del modulo mediale la cui interfaccia/le cui interfacce sono collegate all'anello MRP/HRP viene visualizzata inoltre nella scheda "Interfacce" delle proprietà dell'unità.

Controllo della coerenza - va osservata questa regola

Per l'inserimento rispettare la regola riportata qui di seguito:

- I nomi di domini MRP devono comprendere esclusivamente lettere minuscole, numeri e il carattere "-". I nomi devono iniziare e finire con una lettera minuscola o un numero.

Vedere anche

Controlli di coerenza (Pagina 61)

3.2.7 Particolarità della modalità Ghost

S602 ≥V3.1

Significato

In modalità Ghost l'unità Security non ha un indirizzi IP proprio né sull'interfaccia interna, né sull'interfaccia esterna. Durante il tempo di esecuzione l'unità Security invece rileva l'indirizzo IP per la propria interfaccia esterna da un nodo collegato all'interfaccia interna dell'unità Security e i cui parametri di indirizzo IP possono essere sconosciuti al momento della progettazione. Non è possibile una modifica dell'indirizzo IP del nodo interno e una modifica di indirizzo IP correlato sull'interfaccia esterna. Poiché il nodo interno viene identificato in base al suo indirizzo MAC, le modifiche di indirizzo IP vengono eseguite solo per gli indirizzi MAC appresi. Sull'interfaccia interna dell'unità Security non viene progettato o rilevato nessun indirizzo IP.

In base agli indirizzi MAC l'unità Security scambia l'indirizzo MAC del nodo interno con l'indirizzo MAC dell'unità Security in tutti i pacchetti di dati in uscita sull'interfaccia esterna (risposte del nodo interno).

Attivazione della modalità Ghost - Procedimento:

Requisito richiesto: La modalità Ghost può essere selezionata solo se il progetto si trova in modalità estesa.

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica" > "Proprietà...".
3. Selezionare la voce "Modalità Ghost" nella scheda "Interfacce" dalla casella di riepilogo "Routing interfaccia esterno/interno".

Proprietà dell'unità progettabile

In modalità Ghost sono progettabili tutte le proprietà dell'unità delle seguenti schede:

- Interfacce
- Firewall
- Sincronizzazione dell'ora
- Impostazioni Log
- SNMP

Poiché in modalità Ghost non possono essere progettati server DNS, non è possibile una risoluzione FQDN.

Presupposto per il riconoscimento di un nodo interno

L'unità Security può rilevare l'indirizzo IP del nodo interno solo se il nodo interno ha inizializzato una comunicazione di dati con un partner di comunicazione della rete esterna. L'unità Security non offre inoltre servizi server durante il rilevamento dell'indirizzo IP. Solo dopo che dal nodo interno sono stati inviati pacchetti di dati all'unità Security, l'unità Security può rispondere alle richieste dall'esterno.

Assegnazione della porta per i collegamenti di dati in ingresso e in uscita

Poiché l'interfaccia esterna dell'unità Security e il nodo interno dispongono dello stesso indirizzo IP, deve essere eseguito un indirizzamento mirato dei componenti di rete tramite le porte TCP/UDP. Le porte sono quindi assegnate o all'unità Security o al nodo interno. Nelle seguenti tabelle sono rappresentate le assegnazioni delle porte ai rispettivi apparecchi per i collegamenti di dati in ingresso e in uscita:

Tabella 3- 6 Assegnazione della porta per collegamenti in ingresso (dall'esterno all'unità Security)

Servizio	Porta	Protocollo	Commento
Servizi Web, accesso di progettazione e di diagnostica	443	TCP	La porta HTTPS è sempre attivata e non modificabile per l'accesso di progettazione e di diagnostica tramite il Security Configuration Tool.
SNMP	161	TCP UDP	Dopo l'attivazione di SNMP nel Security Configuration Tool le richieste SNMP in ingresso vengono trasmesse tramite la porta UDP 161. Una trasmissione tramite la porta TCP 161 è inoltre possibile per poter raggiungere ad es. il nodo interno. **Avvertenza** Dopo l'attivazione di SNMP la porta SNMP è assegnata in modo fisso all'unità Security. Se SNMP non è attivato, con l'aiuto di una regola firewall è possibile accedere al nodo interno tramite SNMP.

Tabella 3- 7 Assegnazione della porta per collegamenti in uscita (dall'unità Security verso l'esterno)

Servizio	Porta	Protocollo	Commento
Syslog	514	UDP	Se il servizio Syslog nel Security Configuration Tool è attivato, i messaggi Syslog vengono trasmessi dall'unità Security tramite la porta UDP 514. Questa assegnazione di porta non può essere modificata.
NTP	123	UDP	Se per la sincronizzazione dell'ora vengono utilizzati server NTP, le richieste NTP vengono trasmesse tramite la porta UDP 123. Questa assegnazione di porta non può essere modificata.

Indirizzi IP e maschere della sottorete riconoscibili

L'unità Security riconosce esclusivamente nodi interni che presentano indirizzi IP nell'area delle classi di rete A, B o C. La maschera della sottorete viene rilevata dall'unità Security in base alla relativa classe di rete (vedere tabella "Classi di rete e relative maschere della sottorete"). Per poter rilevare in modo corretto la maschera della sottorete, per il nodo interno deve essere inserito un router standard.

I nodi con indirizzi IP delle classi di rete D e E vengono respinti dall'unità Security.

Tabella 3- 8 Classi di rete e relative maschere della sottorete

Classe di rete	Indirizzi IP		Finestra della sotto-rete
	Limite inferiore	Limite superiore	
A	0.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	Viene respinto dall'unità Security
E	240.0.0.0	255.255.255.255	Viene respinto dall'unità Security

Struttura d'insieme

Viene riconosciuto al massimo un nodo interno dell'unità Security. In caso di diversi nodi interni l'unità Security si comporta nel modo seguente:

- Il primo dispositivo riconosciuto dall'unità Security nella rete interna ottiene l'accesso al segmento di rete esterno se il firewall è configurato in modo corrispondente.
- Il traffico di dati di eventuali altri nodi esistenti nell'area interna della rete viene bloccato partendo dal livello 2 (livello MAC) in base all'indirizzo del mittente.

Caricamento delle configurazioni e della diagnostica dopo la messa in servizio

Dopo il rilevamento di un indirizzo IP da un nodo interno l'unità Security sull'interfaccia esterna dispone di un indirizzo IP che può essere diverso dall'indirizzo IP con il quale l'unità Security è stata inizialmente progettata. Per una modifica della configurazione o per motivi di diagnostica, nel Security Configuration Tool per l'interfaccia esterna è necessario sostituire l'indirizzo IP progettato inizialmente, che l'unità Security ha rilevato dal nodo interno durante l'esecuzione.

Informazioni di routing per le reti gerarchiche sulla porta esterna

Se sull'interfaccia esterna dell'unità Security si trovano reti gerarchiche con accoppiamenti ad altre sottoreti, l'unità Security deve rilevare le relative informazioni di routing dal nodo interno. A tal fine il nodo interno deve rispondere alle richieste ICMP configurate. Non sono necessarie risposte a ICMP Broadcast.

Progettazione di firewall

4

Significato

La funzionalità firewall delle unità Security ha il compito di proteggere le reti e le stazioni da influenze esterne e disturbi. Ciò significa che determinate relazioni di comunicazione precedentemente definite vengono consentite. I telegrammi non autorizzati che non inviano una risposta vengono respinti dal firewall.

Per filtrare il traffico dei dati è inoltre possibile utilizzare indirizzi IP, sotto-reti IP, numeri di porte o indirizzi MAC.

La funzionalità firewall può essere configurata per i seguenti livelli di protocollo:

- IP Firewall con Stateful Packet Inspection (layer 3 e 4)
- Firewall anche per telegrammi Ethernet-"Non-IP" secondo IEEE 802.3 (layer 2)

Il firewall può essere utilizzato per il traffico di dati codificato (tunnel IPsec) e il traffico di dati non codificato.

Regole firewall

Le regole firewall descrivono in quali pacchetti sono consentiti o vietati in quale direzione. Le regole IP hanno effetto su tutti i pacchetti IP del livello 3. Le regole MAC hanno effetto solo su frame al di sotto del livello 3.

Regole firewall automatiche per collegamenti STEP 7

Per i collegamenti progettati in STEP 7, in SCT vengono create automaticamente regole firewall che abilitano il partner di comunicazione. In questa fase vengono osservate le direzioni di realizzazione dei collegamenti.

Le regole sono visibili e possono essere modificate solo in modalità estesa.

Progettazione

Vanno distinti le due visualizzazioni di comando:

- Nella modalità standard si accede a regole firewall semplici predefinite. È possibile abilitare solo regole specifiche per il servizio. I servizi abilitati sono ammessi per tutti i nodi e per la direzione indicava viene consentito l'accesso completo.
- Nella modalità estesa è possibile eseguire le impostazioni firewall. Per un singolo nodo possono essere abilitati singoli servizi o per i nodi possono essere abilitati tutti i servizi per l'accesso alla stazione o alla rete.

  In modalità estesa vanno distinte le seguenti regole firewall e i seguenti set di regole firewall:

  – Le regole firewall locali sono assegnate rispettivamente ad un'unità Security. Esse vengono progettate nella finestra di dialogo delle proprietà dell'unità Security.
  – I set di regole globali del firewall possono essere assegnati contemporaneamente a diverse unità Security. Essi vengono visualizzati e progettati globalmente in modalità estesa nell'area di navigazione del Security Configuration Tool.
  – I set di regole IP pesonalizzati possono essere assegnati contemporaneamente a diverse unità Security. Essi vengono visualizzati e progettati globalmente in modalità estesa nell'area di navigazione del Security Configuration Tool.
    SCALANCE S V4 (RADIUS): Oltre a singoli o più utenti, ai set di regole IP personalizzati possono essere assegnati anche singoli o diversi ruoli.

Inoltre esiste la possibilità di definire in modo chiaro e compatto le regole del firewall con l'aiuto delle definizioni del servizio. Le definizioni di servizi possono essere impiegate in tutti i tipi di regole elencati.

Attivazione firewall

Il firewall viene controllato in modalità standard mediante attivazione della casella opzione "Attiva firewall". Se si disattiva la casella di controllo, le impostazioni firewall inserite continuano ad essere visualizzate nell'elenco, ma non possono essere modificate. Se l'unità Security si trova in un gruppo VPN, come standard la casella di controllo è attivata e non può essere disattivata.

Attivazione delle impostazioni di logging

In modalità standard è possibile attivare il logging globale nella scheda "Firewall". In questo modo tuttavia non vengono visualizzati tutti i pacchetti che attraversano i firewall.

In modalità estesa è possibile attivare il logging per ciascuna singola regola firewall. In questo modo viene eliminata la limitazione riguardo ai pacchetti visualizzati dalla modalità Standard.

Nota

Firewall di SCALANCE S627-2M

Le porte del modulo mediale di SCALANCE S627-2M sono collegate alle porte fisse della relativa interfaccia tramite un blocco switch. Tra le porte stesse dell'interfaccia esterna e tra le porte stesse dell'interfaccia interna non è quindi garantita la funzionalità firewall (Layer 2 / Layer 3).

4.1 CP in modalità standard

Attivazione delle regole del filtro pacchetto

Se in STEP 7 per i CP si attiva la funzione Security, sono dapprima ammessi tutti gli accessi al e tramite il CP. Per attivare singole regole filtro pacchetto fare clic sulla casella di controllo "Attiva firewall". Abilitare successivamente i servizi desiderati. Le regole firewall create automaticamente a causa di una progettazione del collegamento hanno priorità superiore rispetto ai servizi qui impostati. Tutti i nodi hanno accesso ai servizi abilitati.

Impostazioni firewall dettagliate nella modalità estesa

In modalità estesa è possibile limitare le regole firewall a singoli nodi. Per passare in modalità estesa fare clic sulla casella opzione "Modalità estesa".

Nota

Non è possibile una ricommutazione alla modalità standard

Una commutazione nella modalità estesa per il progetto attuale non può più essere annullata.

Progettazione del firewall con VPN

Se l'unità Security si trova in un gruppo VPN, come standard è attivata la casella di controllo "Solo comunicazione via tunnel". Ciò significa che che tramite l'interfaccia esterna non può passare nessuna comunicazione sul tunnel e che è ammesso solo il trasferimenti dei dati IPsec codificato. La regola firewall "Drop" > "Any" > "Esterno" viene creata automaticamente.

Se si disattiva la casella di controllo, sono autorizzate la comunicazione via tunnel e anche i tipi di comunicazione selezionati nelle altre caselle di selezione.

4.1.1 CP x43-1-Adv.

4.1.1.1 Preimpostazione del firewall

Comportamento con preimpostazione

I seguenti diagrammi illustrano dettagliatamente le impostazioni standard rispettivamente per il filtro pacchetto IP e il filtro pacchetto MAC, se la casella di controllo "Attiva firewall" è attivata e anche in modalità estesa non esiste nessuna regola. Il comportamento può essere modificato creando regole firewall corrispondenti in modalità estesa.

Impostazione standard per CP x43-1 Adv.

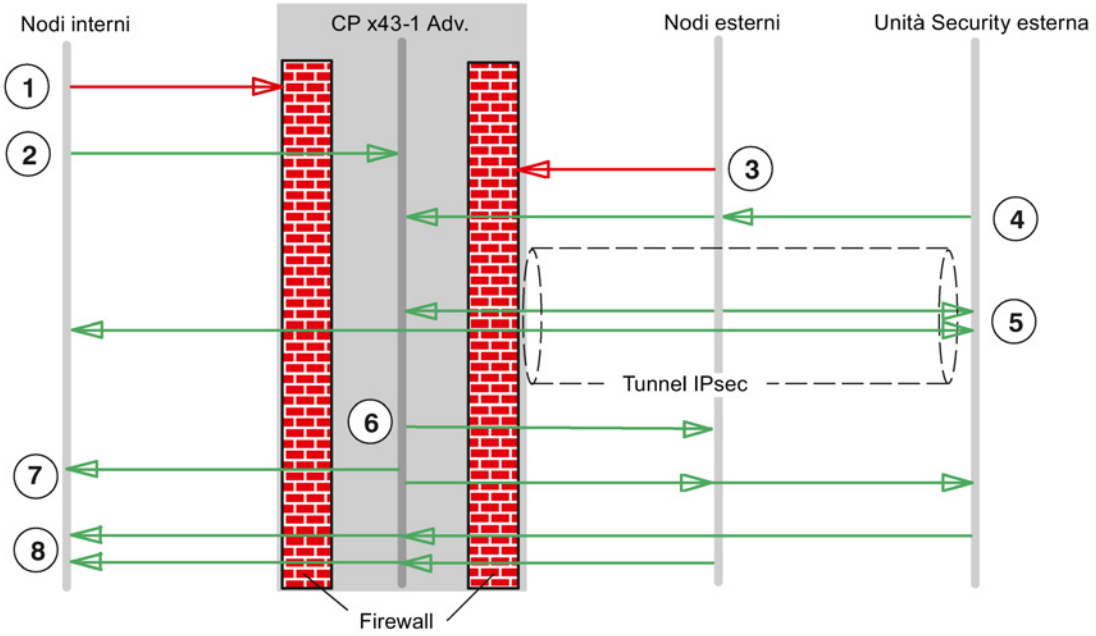


Figura 4-1 Impostazione standard per filtro pacchetto IP CP x43-1 Adv.

① Tutti i tipi di telegramma dall'interno all'esterno sono bloccati.

② Tutti i telegrammi dall'interno all'unità Security sono autorizzati.

③ Tutti i telegrammi dall'esterno all'interno e all'unità Security sono bloccati (anche ICMP Echo Request).

④ Sono autorizzati telegrammi dall'esterno (nodi esterni e unità Security esterni) all'unità Security del seguente tipo:

- Protocollo ESP (codifica)
- IKE (protocollo per la realizzazione del tunnel IPsec)
- NAT-Traversal (protocollo per la realizzazione del tunnel IPsec)

⑤ È autorizzata la comunicazione IP tramite tunnel IPsec.

⑥ I telegrammi del tipo Syslog sono autorizzati verso l'esterno dall'unità Security e non vengono influenzati dal firewall.

Avvertenza

Poiché Syslog è un protocollo non protetto, non è possibile garantire che i dati Log vengano trasmessi in modo protetto.

⑦ Sono autorizzati telegrammi dall'unità Security verso l'interno e verso l'esterno

⑧ Sono ammesse risposte a richieste dalla rete interna o dall'unità Security.

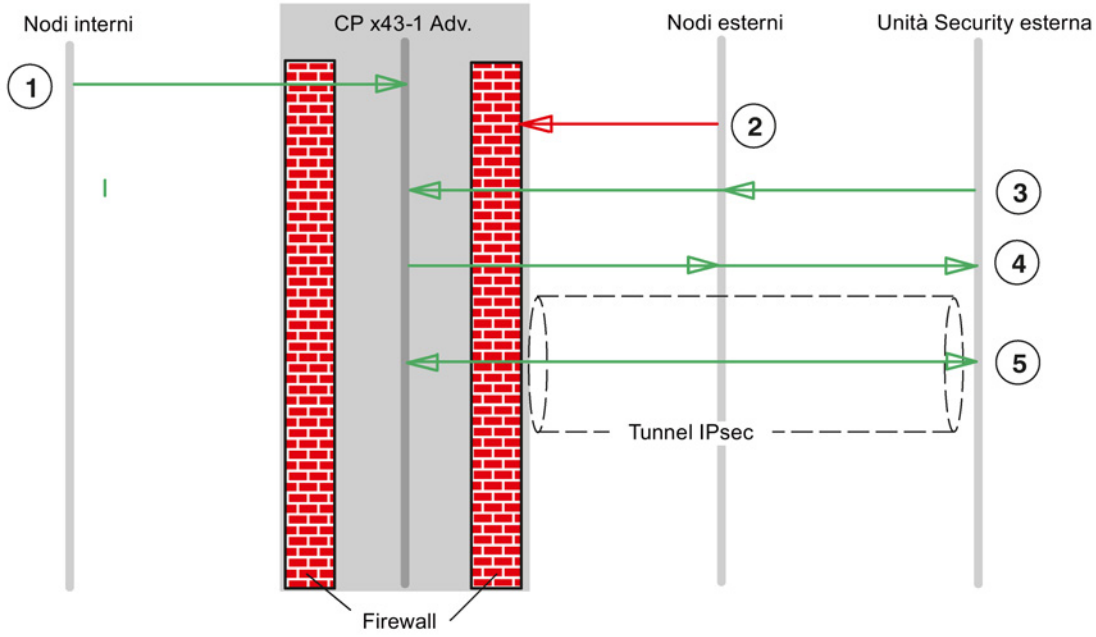


Figura 4-2 Impostazione standard per filtro pacchetto MAC CP x43-1 Adv.

① Tutti i telegrammi dall'interno all'unità Security sono autorizzati.

② Tutti i telegrammi dall'interno all'unità Security sono bloccati.

③ Sono autorizzati tutti telegrammi dall'esterno all'unità Security del seguente tipo:

- ARP con limitazione banda larga
- PROFINET DCP con limitazione banda larga
- LLDP

④ Sono autorizzati telegrammi dall'unità Security all'esterno del seguente tipo:

- ARP con limitazione banda larga
- PROFINET DCP con limitazione banda larga

⑤ Sono autorizzati i seguenti protocolli che vengono inviati attraverso il tunnel IPsec:

- ISO
- LLDP

Nota

Nessuna comunicazione al di fuori dal tunnel VPN

Inoltre, per tutti i partner VPN conosciuti nel progetto viene impedito che possa avvenire una comunicazione tra i punti terminali VPN al di fuori dal tunnel. Il comportamento non può nemmeno essere modificato creando regole firewall corrispondenti in modalità estesa.

4.1.1.2 Progettazione di firewall

A questa funzione si accede nel modo seguente

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "Firewall"

Tabella 4- 1 Servizi e direzioni disponibili

Servizio	Stazione ⇔ esterno Interno ⇒ esterno	Esterno ⇒ interno	Esterno ⇒ stazione	Esterno ⇔ stazione	Porte abilitate	Significato
Comunicazione IP consentita	x	x	x	-	-	Il traffico IP per le direzioni di comunicazione selezionate viene ammesso.
Protocollo S7 consentito	x	x	x	-	Porta TCP 102	Viene ammessa la comunicazione dei nodi di rete tramite il protocollo S7.
Consenti FTP/FTPS (modalità esplicita)	x	x	x	-	Porta TCP 20 Porta TCP 21	Per la gestione dei file e l'accesso ai file tra server e client.
Consenti HTTP	x	x	x	-	Porta TCP 80	Per la comunicazione con un Web server.
Consenti HTTPS	x	x	x	-	Porta TCP 443	Per la comunicazione protetta con un Web Server, ad es. per la diagnostica Web.
Consenti DNS	x	x	-	-	Porta TCP 53 Porta UDP 53	È ammesso il collegamento di comunicazione con un server DNS.
Consenti SNMP	x	x	x	-	Porta TCP 161/162 Porta UDP 161/162	Per la sorveglianza dei nodi di rete con funzione SNMP.
Consenti SMTP	x	x	-	-	Porta TCP 25	Per lo scambio di e-mail tra utenti autenticati e un server SMTP.
Consenti NTP	x	x	-	-	Porta UDP 123	Per la sincronizzazione dell'ora.

Servizio	Stazione ⇔ esterno Interno ⇒ esterno	Esterno ⇒ interno	Esterno ⇒ stazione	Esterno ⇔ stazione	Porte abilitate	Significato
Consenti comunicazione livello MAC	-	-	-	x	-	Il traffico MAC è consentito dall'esterno alla stazione e viceversa.
Consenti comunicazione ISO	-	-	-	x	-	Il traffico ISO è consentito dall'esterno alla stazione e viceversa.

Tabella 4- 2 Logging per set di regole IP e MAC

Set di regole	Operazione in caso di attivazione	Regola creata		
Impostazioni IP Log		Azione	Da	A
Registrazione dei pacchetti via tunnel	Attiva solo se l'unità Security è un nodo di un gruppo VPN. Viene eseguito il logging di tutti i pacchetti IP che sono stati inoltrati via tunnel.	Allow	Stazione	Tunnel
		Allow	Tunnel	Stazione
Registrazione dei pacchetti in ingresso bloccati	Viene effettuato il logging di tutti i pacchetti IP in ingresso che sono stati respinti.	Drop	Esterno	Stazione
Impostazioni MAC Log		Azione	Da	A
Registrazione dei pacchetti in ingresso bloccati verso la stazione	Viene effettuato il logging di tutti i pacchetti MAC in ingresso che sono stati respinti.	Drop	Esterno	Stazione
Registrazione dei pacchetti in uscita bloccati dalla stazione	Viene effettuato il logging di tutti i pacchetti MAC in uscita che sono stati respinti.	Drop	Stazione	Esterno

Nota

Non viene eseguito il loggin del traffico dati tramite i collegamenti progettati.

4.1.1.3 Progettazione dell'elenco degli accessi

Modifica dell'elenco degli accessi IP / delle voci ACL

L'elenco compare se nella scheda protezione di accesso IP di STEP 7 è attivata la casella opzione "Attiva protezione di accesso IP per la comunicazione IP".

Impostare tramite l'elenco di accesso IP la protezione di accesso per determinati indirizzi IP. Le voci dell'elenco già create in STEP 7 vengono visualizzate nell'SCT con i diritti corrispondenti.

Il diritto selezionabile in STEP 7 "Modifica dell'elenco di accesso (M)" non viene trasmesso dopo l'SCT. Per poter trasmettere le autorizzazioni di accesso IP supplementari, nell'SCT è

necessario assegnare all'utente corrispondente il diritto utente "Web: Estendi elenco IP Access Control".

Nota

Comportamento modificato dopo la migrazione

- Dopo la migrazione la protezione di accesso ha ancora effetto solo sull'interfaccia esterna. Per consentire che la protezione di accesso abbia effetto anche sull'interfaccia interna, configurare le regole firewall corrispondenti dall'SCT nella modalità estesa.
- L'unità Security risponde anche alle richieste ARP di indirizzi IP non abilitati (Layer 2).
- Se si migra un elenco IP Access Control senza voci, il firewall viene attivato e al CP non è più possibile accedere dall'esterno. Per consentire che il CP sia raggiungibile, configurare le regole firewall corrispondenti nell'SCT.

A questa funzione si accede nel modo seguente

Voce di menu SCT: Contrassegnare l'unità Security da modificare e selezionare la voce di menu "Modifica " > Proprietà...", scheda "Firewall".

Voce di menu STEP 7: "Protezione di accesso IP" > "Avvio della configurazione firewall", pulsante "Esegui...".

Tabella 4- 3 Indicazioni

Parametri	Significato
Indirizzo IP	Indirizzo IP o area di indirizzi IP consentiti.
Diritti	A seconda dell'assegnazione eseguita. Diritti che non sono abilitati per l'indirizzo IP.
Commento	Inserimento supplementare di un commento.
Logging	Se si attiva la casella di controllo, vengono registrate le regole nel log filtro pacchetto.
Attivazione della modalità estesa	Se si attiva la casella di controllo, vengono convertite le voci nelle seguenti regole firewall.

Tabella 4- 4 Pulsanti

Denominazione	Significato / Effetto
Nuovo...	Creare un nuovo indirizzi IP o una nuova area di indirizzi IP con i relativi diritti.
Modifica...	Selezionare una voce e fare clic su questo pulsante per modificare una voce esistente.
Del	Cancellare la voce selezionata con questo pulsante.

4.1.1.4 Aggiunta di una voce nell'elenco di accesso

Eseguire le seguenti impostazioni

Casella	Descrizione
Indirizzo IP (o inizio dell'area IP)	Inserire l'indirizzo IP o il valore iniziare di un'area di indirizzo IP.
Fine dell'area IP (opzionale)	Inserire il valore finale di un'area di indirizzo IP.
Commento	Inserimenti supplementari di commenti; ad es. per descrivere il partner di comunicazione o l'area di indirizzi.
Questo indirizzo IP è autorizzato per i seguenti accessi	l'accesso alla stazione (A=Access): I partner di comunicazione con indirizzi nell'area di dati indicata hanno accesso alla stazione appartenente al CP (CP / CPU). Questa autorizzazione di accesso è impostata in modo implicito per indirizzi IP indicati nella progettazione del collegamento (valida solo per collegamenti specificati). Routing IP in un'altar sotto-rete (R=Routing): I partner di comunicazione con indirizzi nell'area di dati indicata hanno accesso ad altre sotto-reti collegate al CP (CP / CPU). Questa autorizzazione di accesso non è impostata automaticamente per indirizzi IP indicati nella progettazione del collegamento. In caso di necessità questa autorizzazione di accesso viene impostata esplicitamente.

Ulteriori regole per l'inserimento:

- Viene controllato se vi sono indirizzi singoli multipli; in questo caso vengono riconosciuti: diverse indicazioni singole; sovrapposizione di autorizzazioni.
- Gli indirizzi IP indicati singolarmente possono anche essere presenti all'interno di un'area; valgono quindi le autorizzazione di accesso complessive assegnate ad un indirizzo IP.
- Non viene controllato se un'area contiene indirizzi non validi (ad es. qui possono essere inseriti indirizzi Broadcast sotto-rete, nonostante essi non possano utilizzati come indirizzo IP di un trasmettitore).

4.1.2 CP 1628

4.1.2.1 Preimpostazione del firewall

Comportamento con preimpostazione

I seguenti diagrammi illustrano dettagliatamente le impostazioni standard rispettivamente per il filtro pacchetto IP e il filtro pacchetto MAC, se la casella di controllo "Attiva firewall" è attivata e anche in modalità estesa non esiste nessuna regola. Il comportamento può essere modificato creando regole firewall corrispondenti in modalità estesa.

Impostazione standard per CP 1628

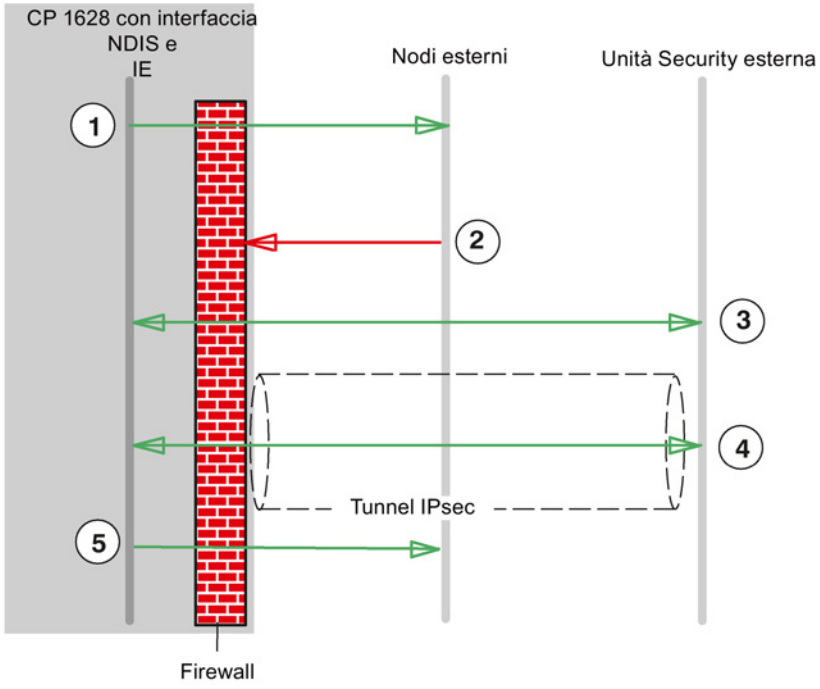


Figura 4-3 Impostazione standard per filtro pacchetto IP CP 1628

① Sono consentiti tutti i telegrammi dall'interfaccia NDIS e IE (Industrial Ethernet) all'esterno.

② Sono bloccati tutti i telegrammi dall'esterno.

③ Sono autorizzati tutti telegrammi dall'esterno all'unità Security e viceversa del seguente tipo:

- Protocollo ESP (codifica)
- IKE (protocollo per la realizzazione del tunnel IPsec)
- NAT-Traversal (protocollo per la realizzazione del tunnel IPsec)

④ È autorizzata la comunicazione IP tramite tunnel IPsec.

⑤ I telegrammi del tipo Syslog sono autorizzati dall'unità Security verso l'esterno.

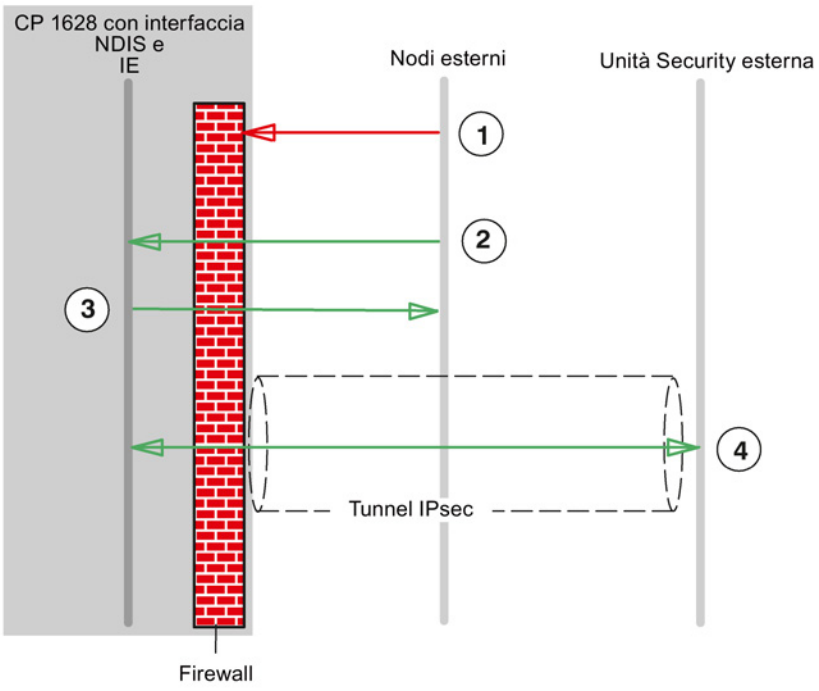


Figura 4-4 Impostazione standard per filtro pacchetto MAC CP 1628

① Sono bloccati tutti i telegrammi dall'esterno.

② Sono autorizzati tutti i telegrammi dall'esterno del seguente tipo:

- ARP con limitazione banda larga
- PROFINET DCP con limitazione banda larga

③ Sono autorizzati telegrammi dall'unità Security all'esterno del seguente tipo:

- PROFINET DCP con limitazione banda larga

④ Sono autorizzati i protocolli MAC che vengono inviati attraverso il tunnel IPsec.

Nota

Nessuna comunicazione al di fuori dal tunnel VPN

Inoltre, per tutti i partner VPN conosciuti nel progetto viene impedito che possa avvenire una comunicazione tra i punti terminali VPN al di fuori dal tunnel. Il comportamento non può nemmeno essere modificato creando regole firewall corrispondenti in modalità estesa.

4.1.2.2 Progettazione di firewall

A questa funzione si accede nel modo seguente

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "Firewall"

Tabella 4- 5 Servizi e direzioni disponibili

Servizio	Esterno ⇒ stazione	Esterno ⇔ stazione	Porte abilitate	Significato
Comunicazione IP consentita	x	-	-	Il traffico IP per le direzioni di comunicazione selezionate viene ammesso.
Protocollo S7 consentito	x	-	Porta TCP 102	Viene ammessa la comunicazione dei nodi di rete tramite il protocollo S7.
Consenti FTP/FTPS (modalità esplicita)	x	-	Porta TCP 20 Porta TCP 21	Per la gestione dei file e l'accesso ai file tra server e client.
Consenti HTTP	x	-	Porta TCP 80	Per la comunicazione con un Web server.
Consenti HTTPS	x	-	Porta TCP 443	Per la comunicazione protetta con un Web Server, ad es. per la diagnostica Web.
Consenti DNS	x	-	Porta TCP 53 Porta UDP 53	È ammesso il collegamento di comunicazione con un server DNS.
Consenti SNMP	x	-	Porta TCP 161/162 Porta UDP 161/162	Per la sorveglianza dei nodi di rete con funzione SNMP.
Consenti SMTP	x	-	Porta TCP 25	Per lo scambio di e-mail tra utenti autenticati e un server SMTP.
Consenti NTP	x	-	Porta UDP 123	Per la sincronizzazione dell'ora.
Consenti comunicazione livello MAC	-	x	-	Il traffico MAC è consentito dall'esterno alla stazione e viceversa.
Consenti comunicazione ISO	-	x	-	Il traffico ISO è consentito dall'esterno alla stazione e viceversa.
Consenti SiCLOCK	-	x	-	I telegrammi dell'ora SiCLOCK sono ammessi dall'esterno alla stazione e viceversa.

Tabella 4- 6 Logging per set di regole IP e MAC

Set di regole	**Operazione in caso di attivazione**	**Regola creata**		
Impostazioni IP Log		**Azione**	**Da**	**A**
Registrazione dei pacchetti via tunnel	Attiva solo se l'unità Security è un nodo di un gruppo VPN. Viene eseguito il logging di tutti i pacchetti IP che sono stati inoltrati via tunnel.	Allow	Stazione	Tunnel
		Allow	Tunnel	Stazione
Registrazione dei pacchetti in ingresso bloccati	Viene effettuato il logging di tutti i pacchetti IP in ingresso che sono stati respinti.	Drop	Esterno	Stazione
Impostazioni MAC Log		**Azione**	**Da**	**A**
Registrazione dei pacchetti in ingresso bloccati	Viene effettuato il logging di tutti i pacchetti MAC in ingresso che sono stati respinti.	Drop	Esterno	Stazione
Registrazione dei pacchetti in uscita bloccati	Viene effettuato il logging di tutti i pacchetti MAC in uscita che sono stati respinti.	Drop	Stazione	Esterno

Nota

Non viene eseguito il loggin del traffico dati tramite i collegamenti progettati.

4.2 SCALANCE S in modalità standard

4.2.1 Preimpostazione del firewall

Comportamento con preimpostazione

I seguenti diagrammi illustrano le impostazioni standard in dettaglio rispettivamente per il filtro pacchetto IP e il filtro pacchetto MAC. Il comportamento può essere modificato creando regole firewall corrispondenti in modalità estesa.

Impostazione standard per SCALANCE S602/S612 a partire da V3

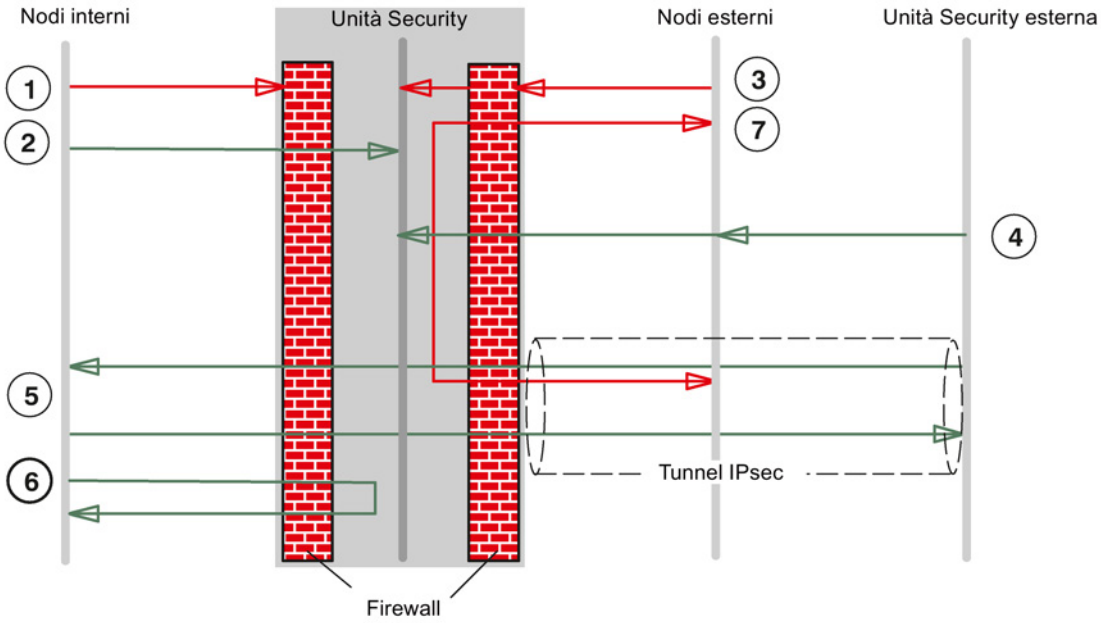


Figura 4-5 Impostazione standard per filtro pacchetto IP SCALANCE S602/S612 a partire da V3

① Tutti i tipi di telegramma dall'interno all'esterno sono bloccati.

② Tutti i telegrammi dall'interno all'unità Security sono autorizzati.

③ Tutti i telegrammi dall'esterno all'interno e all'unità Security sono bloccati.

④ Sono autorizzati telegrammi dall'esterno (nodi esterni e unità Security esterne) all'unità Security del seguente tipo:

- HTTPS (SSL)
- Protocollo ESP (codifica)
- IKE (protocollo per la realizzazione del tunnel IPsec)
- NAT-Traversal (protocollo per la realizzazione del tunnel IPsec)

⑤ È autorizzata la comunicazione IP tramite tunnel IPsec. S602

⑥ Sono ammessi telegrammi dall'interno verso l'esterno.

⑦ I telegrammi dall'esterno sul tunnel all'interfaccia esterna e viceversa sono bloccati. S602

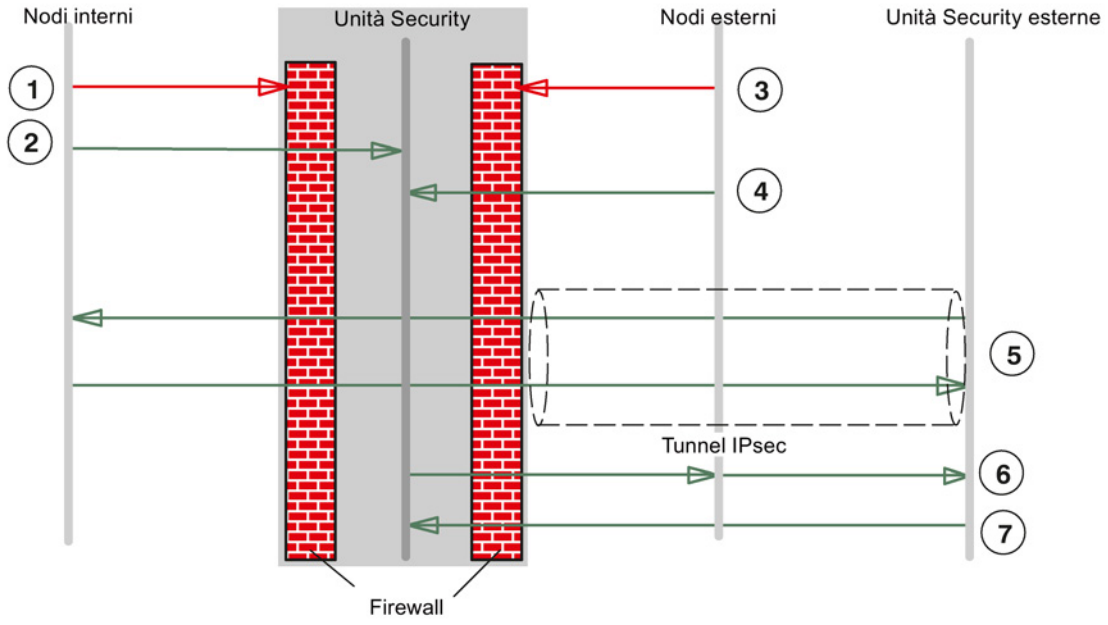


Figura 4-6 Impostazione standard per filtro MAC SCALANCE S602/612 a partire da V3

① Tutti i tipi di telegramma dall'interno all'esterno tranne i seguenti tipi di telegramma sono bloccati.

- Telegrammi ARP

② Tutti i telegrammi dall'interno all'unità Security sono autorizzati.

③ Tutti i telegrammi dall'esterno all'interno tranne i seguenti tipi di telegramma sono bloccati.

- Telegrammi ARP con limitazione banda larga

④ Sono autorizzati telegrammi dall'esterno all'unità Security del seguente tipo:

- ARP con limitazione banda larga
- PROFINET DCP con limitazione banda larga
- In modalità Routing: Telegrammi LLDP (Ethertype 0x88CC) S≥V4.0

⑤ In modalità Bridge: Sono autorizzati i protocolli MAC che vengono inviati attraverso il tunnel IPsec.

⑥ Sono autorizzati telegrammi dall'unità Security all'esterno del seguente tipo:
- PROFINET
- In modalità Routing: Telegrammi LLDP (Ethertype 0x88CC) S≥V4.0

⑦ Sono autorizzati telegrammi Multicast e Broadcast dall'esterno all'unità Security del seguente tipo:
- PROFINET con limitazione della larghezza di banda

Nota

Abilitazione automatica dei tipi Ether

Se PPPoE è attivo, i tipi Ether 0x8863 e 0x8864 vengono abilitati automaticamente (PPPoE Discovery e Session Stage).

Impostazione standard per SCALANCE S623 a partire da V3 e S627-2M V4

Le regole firewall standard per l'interfaccia esterna ed interna corrispondono a quelle valide per le unità SCALANCE S del tipo S602 e S612. Nei seguenti due grafici sono illustrate solo le regole filtro pacchetto IP che riguardano l'interfaccia DMZ. Le regole pacchetto filtro MAC non possono essere definite per l'interfaccia DMZ in quanto i telegrammi tra la rete esterna o interna e l'interfaccia DMZ vengono instradati.

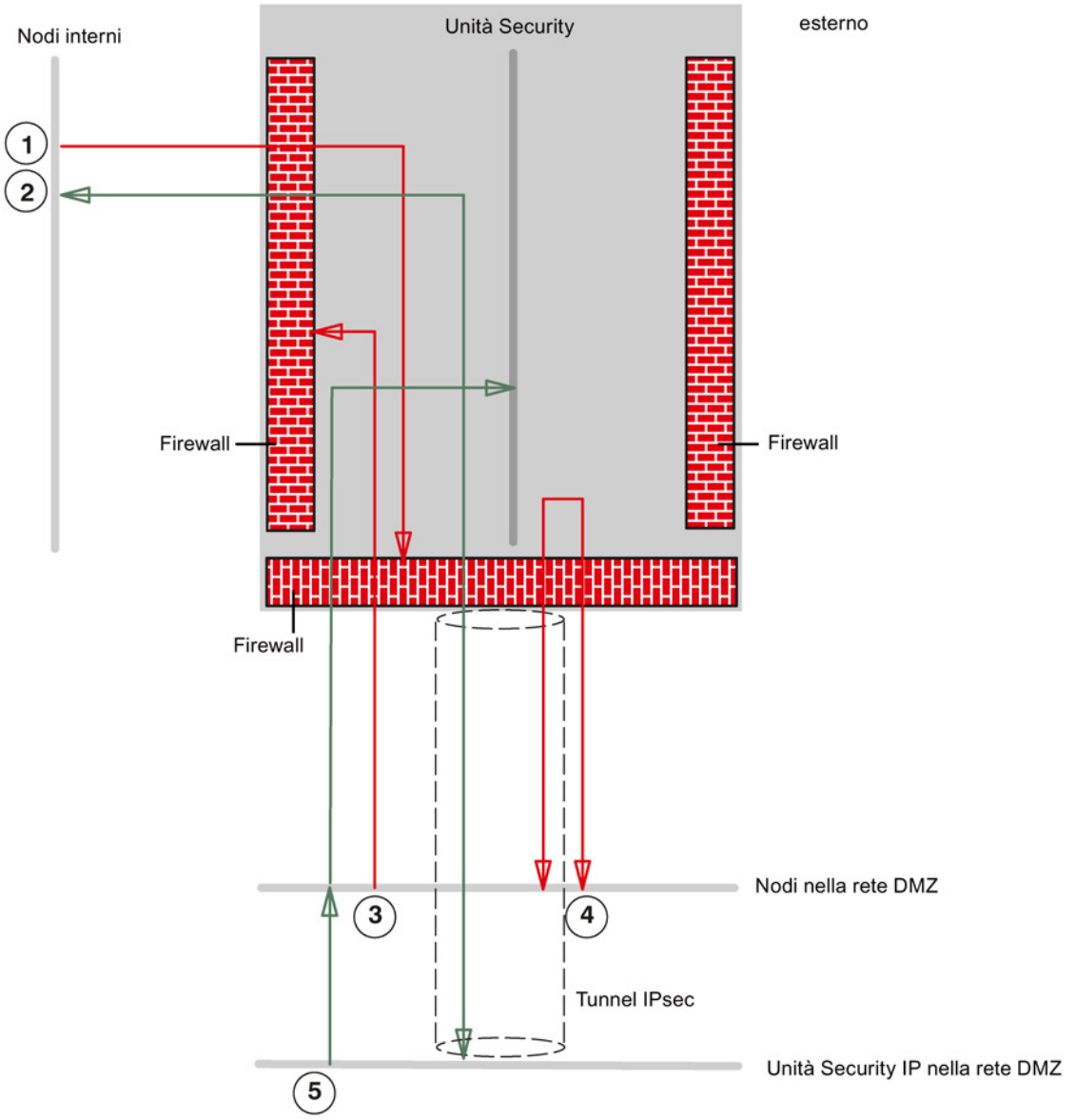


Figura 4-7 Impostazione standard per filtro pacchetto IP SCALANCE S623/S627-2M (traffico tra la rete DMZ e la rete interna o la rete DMZ e l'unità Security)

①Tutti i telegrammi dall'interno alla rete DMZ sono bloccati.

②Sono autorizzati tutti i telegrammi dall'interno verso il tunnel sull'interfaccia DMZ e viceversa

③Tutti i telegrammi dalla rete DMZ verso l'interno sono bloccati.

④Tutti i telegrammi dalla rete DMZ al tunnel sull'interfaccia DMZ e viceversa sono bloccati.

⑤Sono autorizzati i telegrammi del seguente dalla rete DMZ (nodi nella rete DMZ e unità Security nella rete DMZ) sull'unità Security:

- HTTPS (SSL)
- Protocollo ESP (codifica)
- IKE (protocollo per la realizzazione del tunnel IPSec)
- NAT-Traversal (protocollo per la realizzazione del tunnel IPsec)

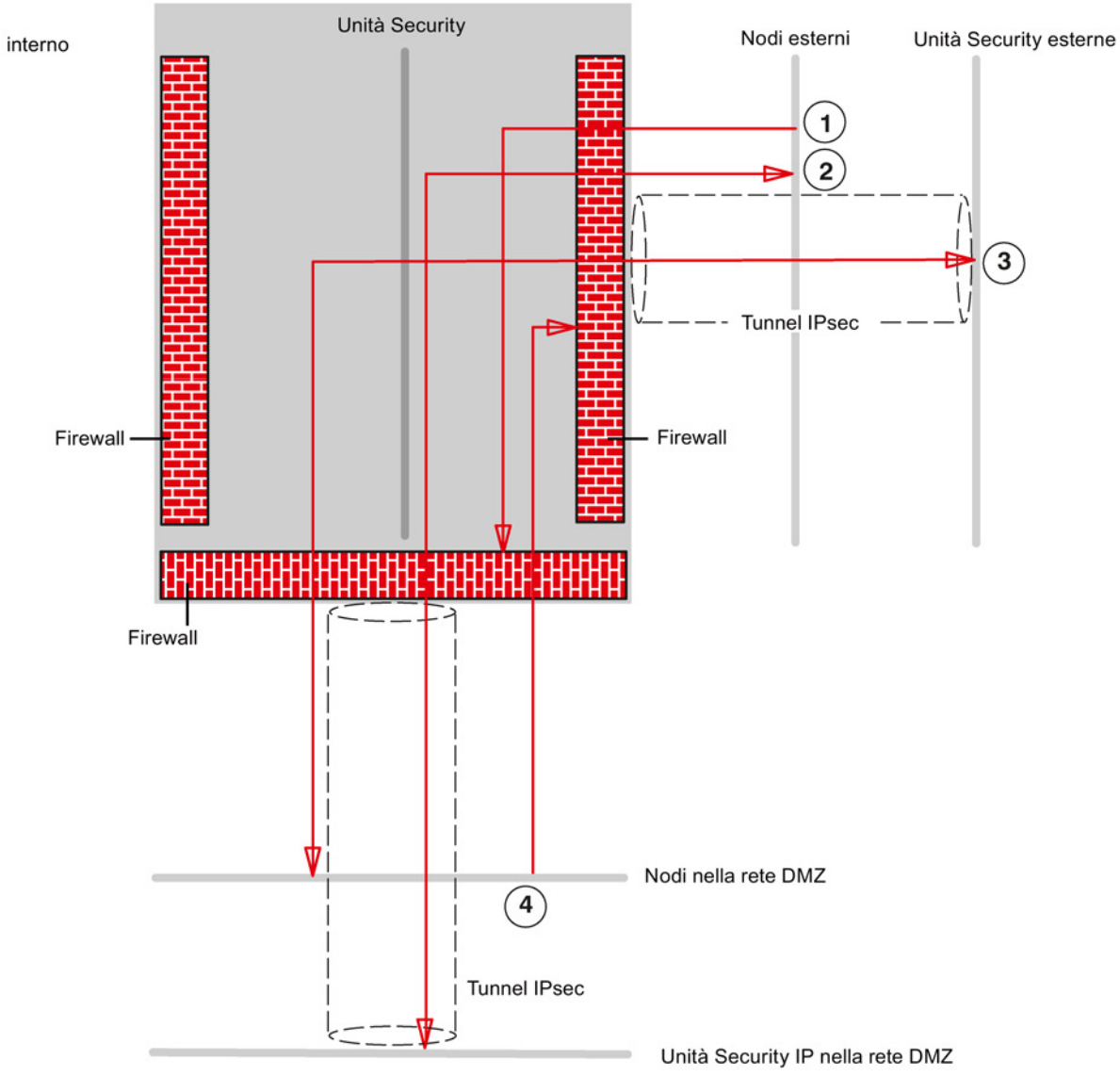


Figura 4-8 Impostazione standard per filtro pacchetto IP SCALANCE S623/S627-2M (traffico tra rete DMZ e rete esterna)

① Tutti i telegrammi dall'esterno alla rete DMZ sono bloccati.

② Sono bloccati tutti i telegrammi dall'esterno verso il tunnel sull'interfaccia DMZ e viceversa

③ Tutti i telegrammi dalla rete DMZ al tunnel sull'interfaccia esterna e viceversa sono bloccati.

④ Sono bloccati tutti i telegrammi dalla rete DMZ all'esterno.

Nota

Abilitazione automatica dei tipi Ether

Se PPPoE è attivo, i tipi Ether 0x8863 e 0x8864 vengono abilitati automaticamente (PPPoE Discovery e Session Stage).

4.2.2 Progettazione del firewall per SCALANCE S ≥ V3.0

A questa funzione si accede nel modo seguente

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "Firewall"

Firewall attivato come standard

Come standard la casella di controllo "Attiva firewall" è attivata. Il firewall è quindi automaticamente attivo e tutti gli accessi dall'esterno all'unità Security sono disabilitati. In modalità Standard facendo clic sulla casella di controllo corrispondente abilitare i firewall per le rispettive direzioni.

Impostazioni firewall dettagliate nella modalità estesa

In modalità estesa è possibile limitare le regole firewall a singoli nodi, vedere il seguente capitolo:

- Firewall in modalità estesa (Pagina 134)

Progettazione del firewall con VPN

Se l'unità Security si trova in un gruppo VPN e in modalità standard è attivata la casella di controllo "Solo comunicazione via tunnel", tramite l'interfaccia esterna o l'interfaccia DMZ è ammasso solo il trasferimento dei dati IPsec codificato. Sul modulo (porta TCP 443) resta possibile solo l'accesso HTTPS senza tunnel.

Se si disattiva la casella di controllo, sono autorizzate la comunicazione via tunnel e anche i tipi di comunicazione selezionati nelle altre caselle di selezione.

Tabella 4- 7 Regole firewall disponibili e direzioni (traffico IP)

Servizio	Interno ⇒ esterno	Esterno ⇒ interno	Interno => DMZ S62x	DMZ => interno S62x	Dall'interno	Dall'esterno	Porte abilitate	Significato
Comunicazione IP consentita	x	x	x	x	-	-	-	La comunicazione IP per le direzioni di comunicazione selezionate viene autorizzata.
Protocollo S7 consentito	x	x	x	x	-	-	Porta TCP 102	Viene ammessa la comunicazione dei nodi di rete tramite il protocollo S7.
Consenti FTP/FTPS (modalità esplicita)	x	x	x	x	-	-	Porta TCP 20 Porta TCP 21	Per la gestione dei file e l'accesso ai file tra server e client.
Consenti HTTP	x	x	x	x	-	-	Porta TCP 80	Per la comunicazione con un Web server.
Consenti HTTPS	x	x	x	x	-	-	Porta TCP 443	Per la comunicazione protetta con un Web Server, ad es. per la diagnostica Web.
Consenti DNS	x	x	x	x	-	-	Porta TCP 53 Porta UDP 53	È ammesso il collegamento di comunicazione con un server DNS.
Consenti SNMP	x	x	x	x	-	-	Porta TCP 161/162 Porta UDP 161/162	Per la sorveglianza dei nodi di rete con funzione SNMP.
Consenti SMTP	x	x	x	x	-	-	Porta TCP 25	Per lo scambio di e-mail tra utenti autenticati e un server SMTP.
Consenti NTP	x	x	x	x	-	-	Porta UDP 123	Per la sincronizzazione dell'ora.
Consenti DHCP	x	x	x	x	-	-	UDP porta 67 UDP porta 68	È ammessa la comunicazione con un server DHCP.

Servizio	Interno ⇒ esterno	Esterno ⇒ interno	Interno => DMZ S62x	DMZ => interno S62x	Dall'interno	Dall'esterno	Porte abilitate	Significato
Consenti comunicazione livello MAC	-	-	-	-	x	x	-	Il traffico MAC è consentito dall'interno all'esterno e viceversa.
Consenti comunicazione ISO	-	-	-	-	x	x	-	Il traffico ISO è consentito dall'interno all'esterno e viceversa.
Consenti SiCLOCK	-	-	-	-	x	x	-	I telegrammi dell'ora SiClock sono ammessi dall'interno verso l'esterno e viceversa.
Consenti DCP	-	-	-	-	x	x	-	Il traffico DCP per l'assegnazione di indirizzi IP è ammesso dall'interno verso l'esterno e viceversa.

Tabella 4- 8 Logging per set di regole IP e MAC

Set di regole	Operazione in caso di attivazione
Impostazioni IP Log	
Registrazione dei pacchetti via tunnel	Attiva solo se l'unità Security è un nodo di un gruppo VPN. Viene eseguito il logging di tutti i pacchetti IP che sono stati inoltrati via tunnel.
Registrazione dei pacchetti in ingresso bloccati	Viene effettuato il logging di tutti i pacchetti IP in ingresso che sono stati respinti.
Registrazione dei pacchetti in uscita bloccati	Viene effettuato il logging di tutti i pacchetti IP in uscita che sono stati respinti.
Impostazioni MAC Log	
Registrazione dei pacchetti via tunnel	Attiva solo se l'unità Security è un nodo di un gruppo VPN. Viene eseguito il logging di tutti i pacchetti MAC che sono stati inoltrati via tunnel.
Registrazione dei pacchetti in ingresso bloccati	Viene effettuato il logging di tutti i pacchetti MAC in ingresso che sono stati respinti.
Registrazione dei pacchetti in uscita bloccati	Viene effettuato il logging di tutti i pacchetti MAC in uscita che sono stati respinti.

4.2.3 Progettazione del firewall per SCALANCE S < V3.0

A questa funzione si accede nel modo seguente

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "Firewall"

Nota

Impostazioni firewall dettagliate nella modalità estesa

In modalità estesa è possibile limitare le regole firewall a singoli nodi.

Nota

Non è possibile una ricommutazione alla modalità standard

Una commutazione nella modalità estesa per il progetto attuale non può più essere annullata.

Rimedio per SCT Standalone: Chiudere il progetto senza salvarlo e aprirlo di nuovo.

Tabella 4- 9 Servizi e direzioni disponibili

Regola/opzione	Porte abilitate	Funzionamento
Solo comunicazione via tunnel	-	Rappresenta l'impostazione standard. L'opzione può essere selezionata solo se l'unità Security si trova in un gruppo VPN. Con questa impostazione viene autorizzato solo il traffico di dati IPsec codificato; possono comunicare tra loro solo nodi protetti dalle unità Security con meccanismi VPN. Se questa opzione è disattivata, è autorizzata la comunicazione via tunnel e inoltre il tipo di comunicazione selezionato nelle altre caselle di selezione.
Consenti comunicazione IP dalla rete interna alla rete esterna	-	I nodi interni possono inizializzare un collegamento di comunicazione con nodi in una rete esterna. Solo i telegrammi di risposta vengono inoltrati dalla rete esterna alla rete interna. Dalla rete esterna non può essere inizializzato nessun collegamento di comunicazione con nodi nella rete interna.
Consenti comunicazione IP con protocollo S7 dalla rete interna alla rete esterna	Porta TCP 102	I nodi interni possono inizializzare un collegamento di comunicazione S7 con nodi in una rete esterna. Solo i telegrammi di risposta vengono inoltrati dalla rete esterna alla rete interna. Dalla rete esterna non può essere inizializzato nessun collegamento di comunicazione con nodi nella rete interna.
Consenti accesso al server DHCP dalla rete interna alla rete esterna	Porta UDP 67 Porta UDP 68	I nodi interni possono inizializzare un collegamento di comunicazione con un server DHCP in una rete esterna. Solo i telegrammi di risposta del server DHCP vengono inoltrati nella rete interna. Dalla rete esterna non può essere inizializzato nessun collegamento di comunicazione con nodi nella rete interna.

Regola/opzione	Porte abilitate	Funzionamento
Consenti accesso al server NTP dalla rete interna alla rete esterna	Porta UDP 123	I nodi interni possono inizializzare un collegamento di comunicazione con un server NTP (Network Time Protocol) in una rete esterna. Solo i telegrammi di risposta del server NTP vengono inoltrati nella rete interna. Dalla rete esterna non può essere inizializzato nessun collegamento di comunicazione con nodi nella rete interna.
Consenti telegrammi dell'ora SiClock dalla rete esterna alla rete interna	-	Con questa opzione vengono abilitati i telegrammi dell'ora SiClock da una rete esterna in una interna.
Consenti accesso al server DNS dalla rete interna alla rete esterna	Porta TCP 53 Porta UDP 53	I nodi interni possono inizializzare un collegamento di comunicazione con un server DNS in una rete esterna. Solo i telegrammi di risposta del server DNS vengono inoltrati nella rete interna. Dalla rete esterna non può essere inizializzato nessun collegamento di comunicazione con nodi nella rete interna.
Consenti la configurazione di nodi di rete tramite DCP	-	Il protocollo DCP viene utilizzato dal tool PST, per eseguire nei componenti di rete SIMATIC NET la denominazione dei nodi (impostazione dei parametri IP). Con questa regola viene consentito ai nodi nella rete esterna di accedere ai nodi nella rete interna tramite protocollo DCP.

Tabella 4- 10 Logging per set di regole IP e MAC

Set di regole	Operazione in caso di attivazione
Impostazioni IP Log	
Registrazione dei pacchetti via tunnel	Solo se l'unità Security è un nodo di un gruppo VPN. Viene eseguito il logging di tutti i pacchetti IP che sono stati inoltrati via tunnel.
Registrazione dei pacchetti in ingresso bloccati	Viene effettuato il logging di tutti i pacchetti IP in ingresso che sono stati respinti.
Registrazione dei pacchetti in uscita bloccati	Viene effettuato il logging di tutti i pacchetti IP in uscita che sono stati respinti.
Impostazioni MAC Log	
Registrazione dei pacchetti via tunnel	Solo se l'unità Security è un nodo di un gruppo VPN. Viene eseguito il logging di tutti i pacchetti MAC che sono stati inoltrati via tunnel.
Registrazione dei pacchetti in ingresso bloccati	Viene effettuato il logging di tutti i pacchetti MAC in ingresso che sono stati respinti.
Registrazione dei pacchetti in uscita bloccati	Viene effettuato il logging di tutti i pacchetti MAC in uscita che sono stati respinti.

4.3 Firewall in modalità estesa

Nella modalità estesa esistono possibilità di impostazione ampliate che consentono l'impostazione individuale delle regole del firmware e della funzionalità di sicurezza.

Commutazione nella modalità estesa

Commutare in modalità estesa per tutte le funzioni descritte in questo capitolo.

Nota

Non è possibile una ricommutazione alla modalità standard

Non appena è stata modificata la configurazione per il progetto attuale, non è più possibile annullare una commutazione nella modalità estesa precedentemente eseguita.

Rimedio SCT Standalone: Chiudere il progetto senza salvarlo e aprirlo di nuovo.

Sono supportati i nomi simbolici

Nelle funzioni descritte di seguito è possibile inserire indirizzi IP o indirizzi MAC anche come nomi simbolici. Per ulteriori informazioni relative ai nodi simbolici vedere il capitolo:

- Impostazione di nomi simbolici per indirizzi IP/MAC. (Pagina 62)

4.3.1 Progettazione del firewall in modalità estesa

Significato

Rispetto alla progettazione di regole del filtro pacchetto preimpostate in modo fisso nella modalità standard, nella modalità ampliata è possibile progettare regole del filtro pacchetto individuali dal Security Configuration Tool.

Le regole del filtro pacchetto si impostato nelle schede selezionabili per i seguenti protocolli:

- Layer 3, 4: Protocollo IP, servizi IP
- Layer 2: Protocollo MAC, servizi MAC

Nota

Nessuna regola MAC con la modalità Routing attivata

SCA. S

Se per l'unità Security è stata attivata la modalità Routing, le regole MAC non vengono utilizzate (le finestre non sono attive).

Se nelle finestre di dialogo descritte di seguito non si inseriscono regole, valgono le impostazioni standard del firewall. I dettagli su questo argomento si trovano nel seguente capitolo:

- Impostazioni standard di CP x43-1 Adv.: Preimpostazione del firewall (Pagina 114)
- Impostazioni standard di CP 1628: Preimpostazione del firewall (Pagina 119)
- Impostazioni standard di SCALANCE S: Preimpostazione del firewall (Pagina 124)

Definizione globale specifica per l'utente e definizione locale possibili

- I set di regole globali del firewall possono essere assegnati contemporaneamente a diverse unità Security. Essi vengono visualizzati e progettati globalmente in modalità estesa nell'area di navigazione del Security Configuration Tool.
- I set di regole IP personalizzati possono essere assegnati contemporaneamente a diverse unità Security. Essi vengono visualizzati e progettati globalmente in modalità estesa nell'area di navigazione del Security Configuration Tool.
  SCALANCE S V4 (RADIUS): Oltre a singoli o più utenti, ai set di regole IP personalizzati possono essere assegnati anche singoli o diversi ruoli.
- Le regole firewall locali sono assegnate rispettivamente ad un'unità Security. Esse vengono progettate nella finestra di dialogo delle proprietà dell'unità Security.

Ad un'unità Security possono essere assegnate diverse regole firewall locali, diversi set di regole firewall globali e diversi set di regole IP personalizzati.

4.3.2 Set di regole firewall globali

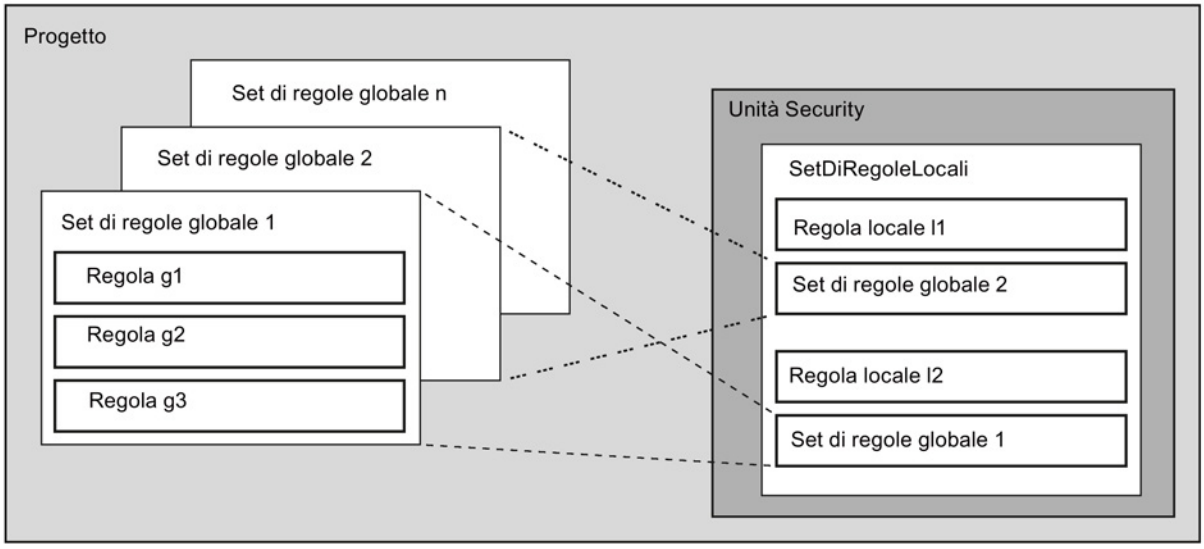
Impiego

I set di regole del firewall globali vengono progettati sul livello del progetto in base all'unità e sono visibili nell'area di navigazione del Security Configuration Tools. Un set di regole firewall globale è costituito da una o diverse regole firewall e viene assegnato a singole unità Security.

Per i set di regole firewall globali si distingue tra:

- Set di regole IP
- Set di regole MAC

La seguente rappresentazione descrive la relazione tra set di regole definiti globalmente e set di regole utilizzati localmente.



Quando si utilizzano set di regole firewall globali?

I set di regole firewall globali vanno utilizzati se per diverse unità Security si vogliono definire criteri di filtri identici per la comunicazione.

Nota

Assegnare solo set di regole firewall supportati dall'unità Security

L'assegnazione errata di set di regole firewall può comportare risultati indesiderati. Controllare quindi sempre le regole firewall locali specifiche per l'unità nel risultato. Un'assegnazione errata non viene riconosciuta durante il controllo automatico della coerenza. Vengono acquisite solo le regole supportate anche dall'unità Security.

Vedere anche

Set di regole IP specifiche per l'utente (Pagina 138)

4.3.2.1 Set di regole firewall globali - Accordi

I set di regole firewall globali vengono utilizzati localmente

I seguenti accordi valgono per la creazione di un set di regole firewall globale e per l'assegnazione ad un'unità:

- Visualizzazione della progettazione

  I set di regole firewall globali possono essere creati solo in modalità estesa.

- Priorità

  Le regole firewall definite localmente hanno come standard una maggiore priorità rispetto ai set di regole firewall globali assegnati localmente. I set di regole firewall globali vengono inseriti quindi in basso nell'elenco delle regole locali.

  La priorità può essere modificata cambiando la posizione nell'elenco delle regole.

- Inserimento, modifica o cancellazione dei set di regole

  I set di regole firewall globali non possono essere editati nell'elenco delle regole locali delle regole firewall nelle proprietà dell'unità. Esse possono essere solo visualizzate e posizionate in base alla priorità desiderata.

  Nell'elenco delle regole locale non può essere cancellata una singola regola firewall di un set regole firewall globale. Dall'elenco delle regole locali può essere cancellato solo l'intero set di regole firewall. Un adattamento del set di regole globale è possibile in qualsiasi momento tramite la finestra di dialogo del set di regole globale.
  Tutti i dispositivi interessati da questa modifica devono successivamente essere ricaricati.

4.3.2.2 Creazione e assegnazione di set di regole firewall globali

A questa funzione si accede nel modo seguente

1. Selezionare nell'area di navigazione una delle seguenti cartelle:
   - "Set di regole firewall globali" > "Set di regole IP firewall".
   - "Set di regole firewall globali" > "Set di regole MAC firewall".
2. Selezionare la voce di menu "Inserisci" > "Set di regole firewall".
3. Inserire i seguenti dati:
   - Nome: Denominazione univoca del set di regole in tutto il progetto. Il nome compare nell'elenco di regole locali dell'unità Security dopo l'assegnazione del set di regole.
   - Descrizione: Inserire la descrizione per il set di regole globali.
4. Fare clic sul pulsante "Aggiungi regola".

5. Inserire nell'elenco la riga dopo la regola firewall. Osservare la descrizione dei parametri nei seguenti capitoli.

   Per i set di regole IP: Regole del filtro pacchetto IP (Pagina 145).

   Per i set di regole MAC: Regole del filtro pacchetto MAC (Pagina 155).

6. Assegnare il set di regole firewall globali alle unità Security nelle quali deve essere utilizzato questo set di regole. Selezionare quindi nell'area di navigazione il set di regole firewall globale e trascinarlo sull'unità Security nell'area di navigazione (Drag and Drop). In alternativa è possibile eseguire l'assegnazione nell'elenco delle regole locali di un'unità Security Security tramite il pulsante "Aggiungi set di regole...".

Risultato

Il set di regole firewall globale viene utilizzato dalle unità Security come set di regole locale e compare automaticamente negli elenchi specifici dell'unità delle regole firewall.

Vedere anche

Set di regole firewall globali - Accordi (Pagina 137)

4.3.3 Set di regole IP specifiche per l'utente

S≥V3.0

Significato

Ai set di regole IP personalizzati vengono dapprima assegnati singoli o diversi utenti. Infine i set di regole IP personalizzati vengono assegnati a singole o diverse unità Security. In questo modo è possibile consentire accessi specifici per l'utente. Se come standard sono ad es. disabilitati tutti gli accessi alle reti dopo un'unità Security, determinati nodi possono essere abilitati temporaneamente tramite i relativi indirizzi IP per un utente. In questo modo per questo utente è consentito l'accesso mentre per gli altri utenti gli accessi restano disabilitati. Le risposte agli accessi personalizzati vengono già consentiti automaticamente. Devono essere progettate solo le regole IP per la direzione dell'iniziativa.

Login dell'utente tramite Internet

L'utente può connettersi all'interfaccia esterna o all'interfaccia DMZ tramite la pagina Web dell'unità Security. Se l'autenticazione è riuscita, viene attivato il set di regole IP definito per l'utente per l'indirizzo IP del dispositivo dal quale è riuscita la connessione.

Il collegamento alla pagina Web dell'unità Security avviene tramite HTTPS utilizzando l'indirizzo IP della porta collegata osservando le regole routing valide:

Esempio:

Interfaccia esterna: 192.168.10.1

Richiamo della pagina di login tramite: https://192.168.10.1/

Gli utenti possono eseguire il login con ciascun ruolo, se l'utente o il ruolo sono assegnati ad un set di regole personalizzato.

Possibilità per l'autenticazione dell'utente

A seconda del metodo di autenticazione selezionato durante la creazione dell'utente che esegue il login all'unità Security, l'autenticazione viene eseguita da diverse istanze:

- Metodi di autenticazione "Password": L'autenticazione viene acquisita dall'unità Security.
- Metodo di autenticazione "RADIUS": L'autenticazione viene acquisita da un server RADIUS. S≥V4.0

Assegnazione di ruoli a set di regole IP personalizzati S≥V4.0

Alle unità SCALANCE S a partire da V4 possono essere assegnati anche set di regole IP personalizzati ai quali sono assegnati ruoli. In questo modo è possibile abilitare un gruppo di utenti per l'accesso a determinati indirizzi IP.

Se un server RADIUS viene utilizzato per l'autenticazione dell'utente e al set di regole IP personalizzato viene assegnato un ruolo, il server RADIUS può autenticare anche questo tipo di utenti che non sono progettati sull'unità Security. Questi utenti devono essere memorizzati nel server RADIUS o in una banca dati separata e qui essere assegnati al ruolo assegnato al set di regole IP personalizzato in SCT. Questo procedimento ha il vantaggio di poter memorizzare tutti gli utenti solo sul server RADIUS.

Le ulteriori informazioni generali relative all'autenticazione mediante server RADIUS si trova nel seguente capitolo:
Autenticazione mediante server RADIUS (Pagina 75)

I set di regole IP personalizzate vengono utilizzati localmente - Accordi

Valgono gli stessi accordi descritti nel seguente capitolo:

- Set di regole firewall globali - Accordi (Pagina 137)

4.3.3.1 Creazione e assegnazione di set di regole IP personalizzati

A questa funzione si accede nel modo seguente

1. Selezionare nell'area di navigazione la cartella "Set di regole IP personalizzati".
2. Selezionare la voce di menu "Inserisci" > "Set di regole firewall".
3. Inserire i seguenti dati:
   - Nome: Denominazione univoca del set di regole IP personalizzato in tutto il progetto. Il nome compare nell'elenco di regole locali dell'unità Security dopo l'assegnazione del set di regole.
   - Descrizione: Inserire la descrizione per il set di regole IP personalizzato.
4. Fare clic sul pulsante "Aggiungi regola".

5. Inserire in sequenza le regole firewall nell'elenco.
   Osservare la descrizione dei parametri nel seguente capitolo:

   – Regole del filtro pacchetto IP (Pagina 145)

   Osservare le particolarità nelle regole firewall che sono state generate automaticamente da SCT per le regole NAT/NAPT:

   – Relazione tra router NAT/NAPT e firewall specifico per l'utente (Pagina 178)

6. Assegnare al set di regole IP personalizzato un utente o più utenti e/o un ruolo o diversi ruoli. L'assegnazione di ruolo a set di regole IP personalizzati è possibile solo per unità SCALANCE S V4.

Nota

Assegnazione di set di regole IP personalizzate

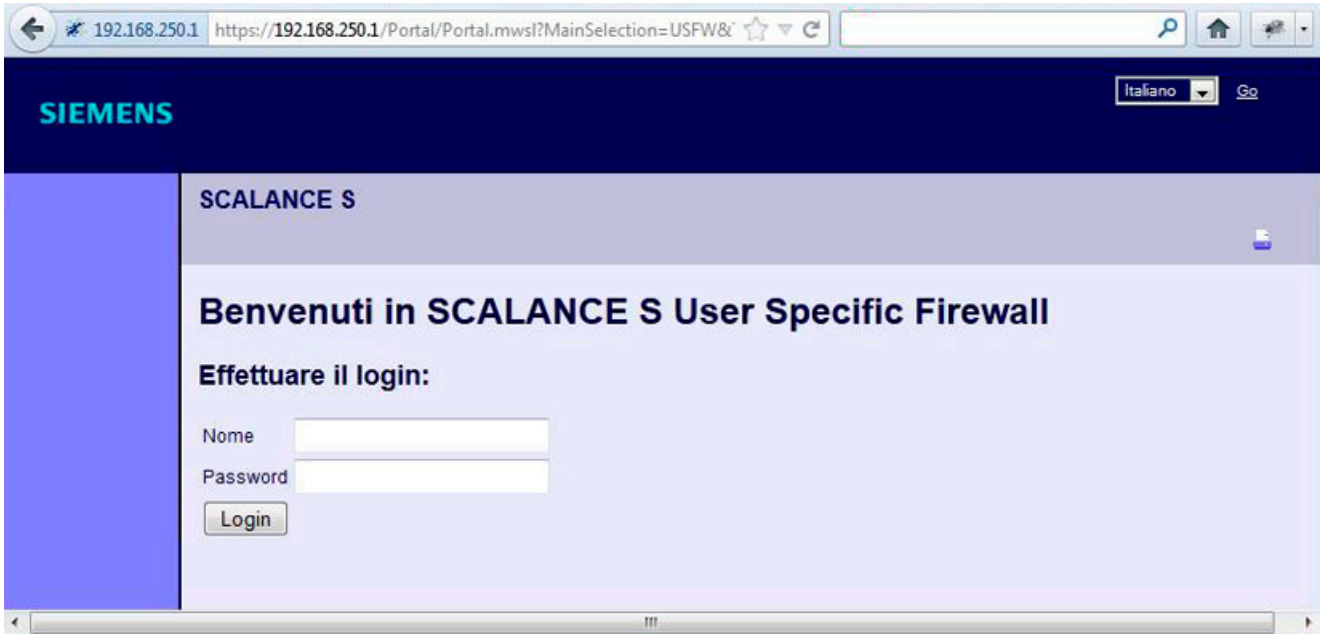
- Ad un'unità Security per ciascun utente può essere assegnato solo un set di regole IP personalizzato.
- Con l'assegnazione per tutti gli utenti o ruoli assegnati al set di regole IP viene attivato implicitamente il diritto "L'utente/il ruolo può eseguire il login all'unità".

---

7. Assegnare il set di regole IP personalizzato alle unità Security nelle quali deve essere utilizzato questo set di regole. Selezionare quindi nell'area di navigazione il set di regole IP personalizzato e trascinarlo sull'unità Security nell'area di navigazione (Drag and Drop). In alternativa è possibile eseguire l'assegnazione nell'elenco delle regole locali di un'unità Security Security tramite il pulsante "Aggiungi set di regole...".

Risultato

- Il set di regole IP personalizzato viene utilizzato dalle unità Security come set di regole locale e compare automaticamente nell'elenco specifico per l'unità delle regole firewall.
- L'utente può effettuare il login all'unità Security. A seconda del metodo di autenticazione, l'autenticazione dell'utente viene eseguita dall'unità Security o da un server RADIUS.



Aree dei valori per la durata massima della sessione

Il tempo dopo il quale l'utente viene disconnesso automaticamente può essere definito durante la creazione o la modifica di un utente ed è come standard di 30 minuti. La durata della sessione può essere prolungata del valore assegnato all'utente nella pagina Web dell'unità Security.

Ulteriori informazioni sulla creazione di utenti si trovano nel seguente capitolo: Gestione degli utenti (Pagina 64)

4.3.4 Regole firewall automaticamente riferite al collegamento

CP

Regole firewall create automaticamente in SCT

Per il seguente caso applicativo vengono create automaticamente regole firewall.

- Collegamenti progettati in STEP 7

Regole firewall per collegamenti progettati

Se in STEP 7 sono creati collegamenti, per questi ultimi in SCT vengono create automaticamente regole firewall. Inoltre ha luogo un reciproco adattamento del sistema tra STEP 7 e SCT nel quale vengono controllati tutti i collegamenti progettati nel progetto. Per ogni partner di comunicazione vengono livellati automaticamente l'indirizzo IP/indirizzo MAC, l'azione e l'interfaccia. Per ciascun partner di comunicazione vi sono 2 regole indipendentemente dal numero dei collegamenti.

Nota

Abilitazione manuale di collegamenti UDP Multicast e UDP Broadcast

Per i collegamenti UDP Multicast e UDP Broadcast non vengono create regole firewall automatiche Per abilitare i collegamenti aggiungere manualmente le regole firewall corrispondenti in modalità estesa.

A seconda della configurazione del collegamento progettata in STEP 7, in SCT vengono creati i seguenti livelli di regole firewall 3. Se l'unità Security si trova in un gruppo VPN, la direzione cambia da "Esterno" a "Tunnel".

Nella colonna "Indirizzo IP sorgente" o "Indirizzo IP di destinazione" di queste regole Firewall viene inserito rispettivamente l'indirizzo IP del partner del collegamento.

CP->esterno	Azione	Da	A
attivo	Allow	Stazione	Esterno
	Drop	Esterno	Stazione
passivo	Drop	Stazione	Esterno
	Allow	Esterno	Stazione
attivo e passivo	Allow	Esterno	Stazione
	Allow	Stazione	Esterno

CP->interno	Azione	Da	A
attivo	Allow	Stazione	Interno
	Drop	Interno	Stazione
passivo	Drop	Stazione	Interno
	Allow	Interno	Stazione
attivo e passivo	Allow	Interno	Stazione
	Allow	Stazione	Interno

Per collegamenti sul livello 2 vengono create regole "Allow" per entrambe le direzioni. Se l'unità Security si trova in un gruppo VPN, la direzione cambia da "Esterno" a "Tunnel".

Nella colonna "Indirizzo MAC sorgente" o "Indirizzo MAC di destinazione" di queste regole Firewall viene inserito rispettivamente l'indirizzo MAC del partner del collegamento.

CP->esterno	Azione	Da	A
attivo, passivo, attivo e passivo	Allow	Stazione	Esterno
	Allow	Esterno	Stazione

Accordi per regole firewall create automaticamente

- Priorità

  Le regole hanno maggiore priorità e vengono quindi inserire in alto nell'elenco di regole locale.

- Cancella regole

  I set di regole non possono essere cancellati. Il logging può essere attivato e i servizi possono essere assegnati. Inoltre è possibile inserire una larghezza di banda e un commento.

- Cambio di azione

  Se in SCT si cambia l'azione da "Allow" a "Drop" e viceversa, queste impostazioni possono essere sovrascritte di nuovo in caso di un nuovo livellamento del sistema. Se le modifiche eseguite devono essere mantenute, selezionare come azione "Allow*" o "Drop*". In questo caso viene livellato solo l'indirizzo IP/indirizzo MAC con STEP 7, l'azione e la direzione vengono mantenute come impostate. Le impostazioni relative al logging, al servizio, alla larghezza di banda e al commento vengono mantenute anche in caso di un nuovo livellamento del sistema, anche senza modifica dell'azione in "Allow*" o "Drop*" . Se in STEP 7 non esiste il collegamento corrispondente, la regola viene cancellata dall'elenco.

Unità Security nel gruppo VPN

Come standard la casella di controllo "Solo comunicazione via tunnel" viene attivata. Disattivando la casella di controllo è possibile creare, oltre alla comunicazione tra i partner del tunnel, la comunicazione con nodi di rete non provvisti di tunnel.

- La comunicazione si svolge fuori dal tunnel se l'indirizzo partner fa parte di una stazione conosciuta nell'SCT, con la quale non è progettato nessun tunnel VPN.
- La comunicazione si svolge attraverso il tunnel VPN se l'indirizzo partner è un punto terminale VPN.
- Se non è possibile assegnare in modo univoco se un collegamento deve essere svolto all'interno o fuori dal tunnel, il collegamento viene assegnato al tunnel VPN e viene visualizzata un'avvertenza corrispondente. L'assegnazione può essere adattata in modalità estesa, ad es. modificando la direzione "Da" "Tunnel" a "Esterno". Per evitare che questo adattamento venga sovrascritto durante un nuovo livellamento del sistema è necessario selezionare l'azione "Allow*" o "Drop*".

Nota

Se deve essere garantita solo una comunicazione attraverso il tunnel, in modalità firewall estesa è possibile creare regole firewall corrispondenti, ad es. per nodi interni o indirizzi NDIS.

Per consentire esclusivamente una comunicazione via tunnel per un CP, inserire una regola con le seguenti impostazioni:

- "Azione": "Drop"
- "Da": "Any"
- "A": "Esterno"

Per il CP 1628 inserire una regola con le seguenti impostazioni:

- "Azione": "Drop"
- "Da": "Stazione"
- "A": "Esterno"

Inoltre è necessario cancellare le regole Firewall già esistenti che consentono una comunicazione senza tunnel.

4.3.5 Impostazione delle regole del filtro pacchetto IP locali

Tramite le regole del filtro pacchetto IP è possibile filtrare sui telegrammi IP come per esempio telegrammi UDP, TCP, ICMP.

All'interno di una regola del filtro pacchetto IP è possibile accedere alle definizioni del servizio e mantenere quindi la limitazione dei criteri di filtraggio. Se non si indicano servizi, la regola del filtro pacchetto IP vale per tutti i servizi.

Si apre la finestra di dialogo delle regole locali del filtro pacchetto IP.

SCT: Contrassegnare l'unità Security da modificare e selezionare la voce di menu "Modifica " > Proprietà...", scheda "Firewall".

STEP 7: Nella scheda "Security" di fianco a "Avvio della configurazione Security" fare clic sul pulsante "Esegui", scheda "Firewall".

Inserire le regole del filtro pacchetto IP

Inserire in sequenza le regole del firewall nell'elenco; osservare la descrizione dei parametri e gli esempi nel seguente capitolo o nella guida in linea.

Utilizzo dei set di regole globali e specifiche per l'utente

I set di regole firewall globali e i set di regole IP personalizzati assegnati all'unità vengono registrati automaticamente nell'elenco di regole locale. Se il set di regole assegnato alla fine dell'elenco di regole, esso viene modificato con la priorità più bassa. La priorità può essere modificata modificando la posizione nell'elenco delle regole.

La guida in linea descrive il significato dei singoli pulsanti.

4.3.6 Regole del filtro pacchetto IP

L'elaborazione delle regole del filtro pacchetto IP avviene in base alle seguenti analisi:

- parametri inseriti nella regola;
- Sequenza e priorità delle regole correlata.

Parametri

La progettazione di una regola IP comprende i seguenti parametri:

Denominazione	Significato / Commento	Possibilità di selezione / campi dei valori
Azione	Definizione delle autorizzazioni (abilitazione/disabilitazione)	• Allow Autorizzazione di telegrammi in base alla definizione. • Drop Disabilitazione di telegrammi in base alla definizione. Per regole del collegamento create automaticamente: CP • Allow* • Drop* Se si selezionano queste regole, non ha luogo nessun livellamento con STEP 7. Le regole modificate non vengono quindi sovrascritte nell'SCT.
Da / A	Le direzioni di comunicazione ammesse.	Viene descritto nella seguente tabella.
Indirizzo IP sorgente	Indirizzo sorgente dei pacchetti IP	Vedere le seguenti sezioni in questo capitolo: • Regole del filtro pacchetto IP (Pagina 145) In alternativa è possibile inserire nomi simbolici. **Avvertenza sulla modalità Ghost** S602 ≥V3.1 Con la modalità Ghost attivata viene rilevato dinamicamente l'indirizzo IP del nodo interno dall'unità Security durante l'esecuzione. A seconda della direzione selezionata non è possibile eseguire inserimenti nella colonna "Indirizzo IP sorgente" (in caso di direzione "Dall'interno verso l'esterno") o nella colonna "Indirizzo IP di destinazioneZ" (in caso di direzione "Dall'esterno verso l'interno"). Al suo posto viene inserito automaticamente l'indirizzo IP nella regola firewall attraverso lo SCALANCE S stesso.
Indirizzo IP di destinazione	Indirizzo di destinazione dei pacchetti IP	
Service	Nome del servizio IP/ICMP o del gruppo di servizi utilizzato. Grazie alle definizioni del servizio possono essere definite le regole filtro pacchetto. Qui si seleziona un servizio definito nella finestra di dialogo dei servizi IP: • Servizi IP • Servizi ICMP • Gruppo di servizi con servizi IP e/o ICMP contenuti Se non si è ancora definito un servizio o se non si intende definire altri servizi, azionare il pulsante "Servizi IP/..." (nella scheda "Regole IP") o "Servizi MAC..." (nella scheda "Regole MAC").	La casella di riepilogo a discesa offre per la selezione i servizi progettati e i gruppi dei servizi. Nessuna indicazione significa: non viene controllato nessun servizio, la regola vale per tutti i servizi. **Avvertenza**: Per visualizzare i servizi IP predefiniti nella casella di riepilogo, attivare prima questi servizi in modalità standard.

Denominazione	Significato / Commento	Possibilità di selezione / campi dei valori
Larghezza di banda (Mbit/s)	Possibilità di impostazione per una limitazione banda larga. Può essere inserita solo se selezionata nell'azione "Allow". Un pacchetto passa dal firewall, quando la regola di pass è giusta e la larghezza di banda ammessa per questa regola non è ancora stata superata.	CP x43-1 Adv. e SCALANCE S < V3.0: 0.001 ... 100 CP 1628 e SCALANCE S ≥ V3.0: 0.001 ... 1000 Per le regole nei set di regole globali e personalizzati: 0.001 ... 100
Logging	Attivazione o disattivazione del logging per questa regola. Le informazioni relative all'impostazione logging si trovano nel seguente capitolo: Registrazione di eventi (logging) (Pagina 253)	
N.	Numeri della regola assegnati automaticamente per l'assegnazione dei pacchetti logging alla regola firewall progettata. Spostando le regole i numero vengono rilevati di nuovo.	
Stateful	Se questa casella di controllo è stata disattivata per una regola IP con l'azione "Allow", tramite i pacchetti ai quali accede la regola Allow non vengono generati States firewall. Tramite gli States firewall le risposte ai pacchetti ammessi vengono consentite automaticamente. Può essere adattata solo se selezionata nell'azione "Allow". La progettazione di regole IP senza States firewall è possibile solo per moduli SCALANCE S a partire dal firmware V3. Se vengono consentite anche le risposte ai pacchetti che devono avere attraversato il firewall secondo le regole IP di questo tipo, per queste risposte è necessario progettare regole IP supplementari.	
Commento	Spazio per la spiegazione della regola.	Se un commento è contrassegnato con "AUTO", esso è stato creato automaticamente per una regola di collegamento.

Tabella 4- 11 Direzioni CP

Possibilità di selezione / campi dei valori		**Unità Security**		**Significato**
Da	**A**	**CP x43-1 Adv.**	**CP 1628**	
Interno	Stazione	**x**	-	Accesso da rete interna a stazione.
	Any	**x**	-	Accesso da una rete interna ad una esterna, al partner tunnel VPN e alla stazione.
Esterno	Stazione	**x**	**x**	Accesso da rete esterna a stazione.
	Any	**x**	-	Accesso da rete esterna a rete interna e alla stazione.
Stazione	Interno	**x**	-	Accesso dalla stazione alla rete interna.
	Esterno	**x**	**x**	Accesso dalla stazione alla rete esterna.
	Tunnel	**x**	**x**	Accesso dalla stazione al partner tunnel VPN.
Tunnel	Stazione	**x**	**x**	Accesso da partner tunnel VPN a stazione.
	Any	**x**	-	Accesso da partner tunnel VPN alla rete interna e alla stazione.
Any	Esterno	**x**	-	Accesso dalla rete interna e dalla stazione alla rete esterna.

Tabella 4- 12 Direzioni SCALANCE S

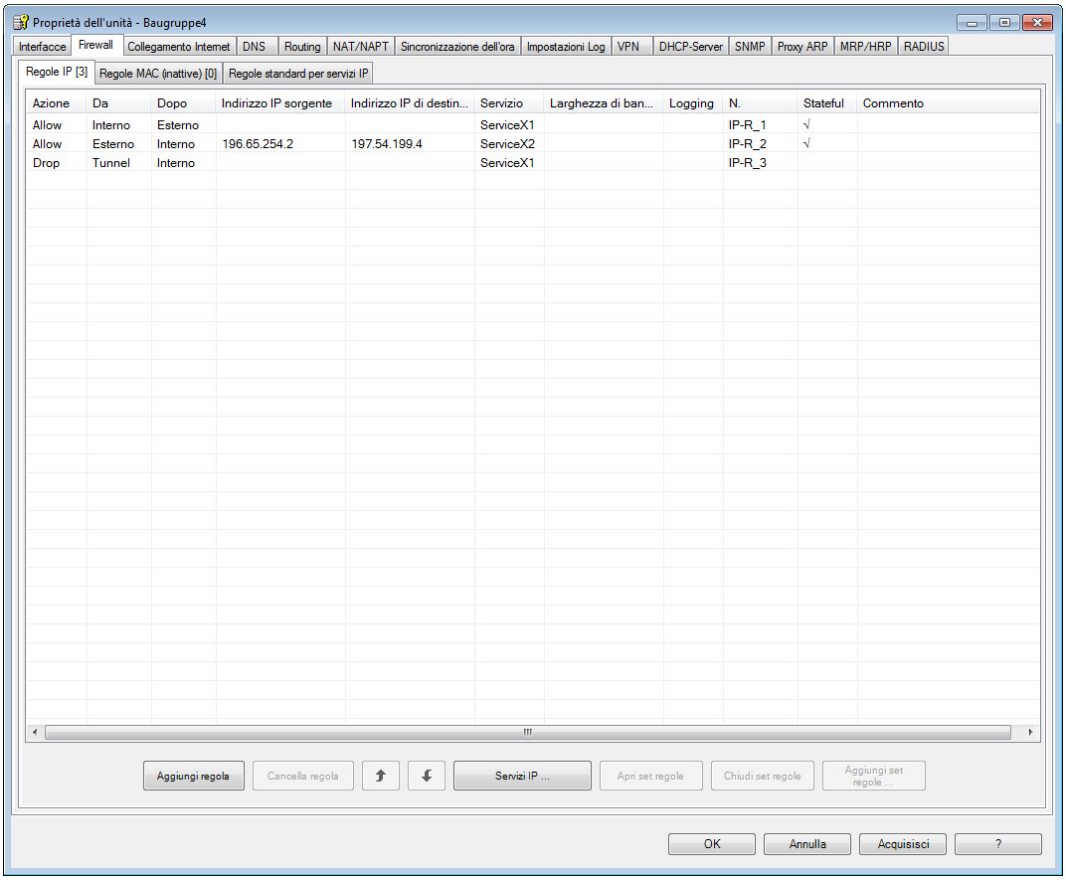
Possibilità di selezione / campi dei valori		**Unità Security**		
Da	**A**	**S602**	**S61x**	**S623 / S627-2M**
Interno	Esterno	**x**	**x**	**x**
	Tunnel	-	**x**	**x**
	Any	-	**x**	**x**
	DMZ	-	-	**x**
	Interno	**x**	**x**	**x**
Esterno	Interno	**x**	**x**	**x**
	Any	-	-	**x**
	Tunnel	-	-	**x**
	DMZ	-	-	**x**
Tunnel	Interno	-	**x**	**x**
	Esterno	-	**x**	**x**
	DMZ	-	**-**	**x**
Any	Interno	-	**x**	**x**
	Esterno	-	-	**x**
	DMZ	-	-	**x**
DMZ	Interno	-	-	**x**
	Esterno	-	-	**x**
	Any	-	-	**x**
	Tunnel	-	-	**x**

Sequenza per l'analisi delle regole con l'unità Security

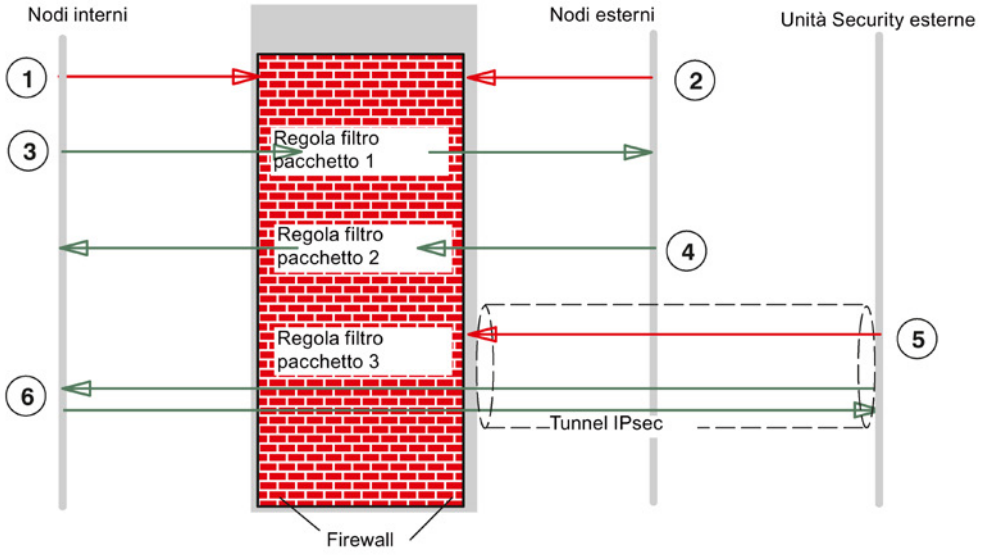
Le regole del pacchetto filtro vengono analizzate nel modo seguente:

- L'elenco viene analizzato dall'alto verso il basso; in caso di regole contradditorie (ad es. voci con le stesse indicazioni di direzione, ma con diverse azioni) vale quindi sempre la voce che si trova più in alto.
- Nelle regole per la comunicazione tra rete interna, rete esterna e rete DMZ vale: tutti i telegrammi, eccetto i telegrammi autorizzati in modo esplicito nell'elenco, sono disabilitati.
- Nelle regole per la comunicazione in direzione di ingresso e di uscita tunnel IPsec vale: tutti i telegrammi, eccetto i telegrammi disabilitati in modo esplicito nell'elenco, sono autorizzati.

Esempio



Le regole filtro pacchetto rappresentate causano il seguente comportamento:



① Tutti i tipi di telegramma dall'interno all'esterno sono bloccati come standard, eccetto quelli autorizzati in modo esplicito.

② Tutti i tipi di telegramma dall'esterno all'interno sono bloccati come standard, eccetto quelli autorizzati in modo esplicito.

③ La regola del filtro pacchetto IP 1 consente i telegrammi con la definizione di servizio "Service X1" dall'interno all'esterno.

④ La regola del filtro pacchetto IP 2 consente i telegrammi dall'esterno all'interno se viene soddisfatta la seguente condizione:

- Indirizzo IP del mittente: 196.65.254.2
- Indirizzo IP del destinatario: 197.54.199.4
- Definizione del servizio: "Service X2"

⑤ La regola del filtro pacchetto IP 3 blocca i telegrammi con la definizione di servizio "Service X1" che vengono inviati dal tunnel VPN alla rete interna.

⑥ Come standard la comunicazione IPsec Tunnel è autorizzata, eccetto i tipi di telegrammi bloccati in modo esplicito.

Vedere anche

Regole del filtro pacchetto MAC (Pagina 155)

Aree dei valori indirizzo IP, maschera della sottorete indirizzo dell'accoppiamento ad altra rete (Pagina 263)

Indirizzi IP nelle regole del filtro pacchetto IP

L'indirizzo IP è composto da 4 numeri decimali dell'area di valori da 0 a 255, divisi tra loro da un punto; esempio: 141.80.0.16

Nella regola del filtro pacchetto esistono le seguenti possibilità per indicare gli indirizzi IP:

- nessuna indicazione

  Non viene eseguito nessun controllo, la regola vale per tutti gli indirizzi IP.

- un indirizzo IP

  La regola vale esattamente per l'indirizzo indicato.

- più indirizzi IP

  La regola vale per tutti gli indirizzi indicati.

  Gli indirizzo vengono indicati separati da un punto e virgola.

- Banda indirizzo

  La regola vale per tutti indirizzi IP che si trovano nella banda di indirizzi.

  Una banda di indirizzi viene definita indicando il numero di posizioni di bit valide nell'indirizzo IP nella seguente forma: [Indirizzo IP]/[Numero dei bit da considerare]

  – [Indirizzo IP]/24 significa quindi che vengono considerati nella regola del filtro solo i 24 bit con valore maggiore dell'indirizzo IP; sono le prime tre posizioni dell'indirizzo IP.

  – [Indirizzo IP]/25 significa che vengono considerati nella regola del filtro solo le prime tre posizioni e il bit con valore maggiore della quarta posizione dell'indirizzo IP.

- Campo di indirizzi

  Per gli indirizzi IP sorgente può essere indicata un''area di indirizzi, separata da un trattino:

  [Indirizzi IP iniziale]-[Indirizzo IP finale]

Maggiori informazioni si trovano nel seguente capitolo:

- Aree dei valori indirizzo IP, maschera della sottorete indirizzo dell'accoppiamento ad altra rete (Pagina 263)

Tabella 4- 13 Esempi per la banda di indirizzi per indirizzi IP

Indirizzo IP sorgente e indirizzo IP di destinazione	**Banda indirizzo**		**Numero indirizzi**
	da	**a**	
192.168.0.0**/16**	192.168.0.0	192.168.255.255	65.536
192.168.10.0**/24**	192.168.10.0	192.168.10.255	256
192.168.10.0**/25**	192.168.10.0	192.168.10.127	128
192.168.10.0**/26**	192.168.10.0	192.168.10.63	64
192.168.10.0**/27**	192.168.10.0	192.168.10.31	32
192.168.10.0**/28**	192.168.10.0	192.168.10.15	16
192.168.10.0**/29**	192.168.10.0	192.168.10.7	8
192.168.10.0**/30**	192.168.10.0	192.168.10.3	4

4.3.7 definizione dei servizi IP

A questa funzione si accede nel modo seguente

- Con il comando di menu "Opzioni " > "Servizi IP...".

  o

- Dalla scheda "Regole IP" con il pulsante "Servizi IP...".

Significato

Con l'aiuto delle definizioni del servizio IP è possibile definire in modo chiaro e compatto le regole del firewall che vengono utilizzate su determinati servizi. Per questo si assegna un nome e si assegnano al nome i parametri del servizio.

Inoltre è possibile riunire in gruppi i servizi definiti in un sottogruppo.

Per la progettazione delle regole del filtro pacchetto globali o locali utilizzare questo nome.

Parametri per servizi IP

La definizione dei servizi IP viene eseguita con i seguenti parametri:

Tabella 4- 14 Servizi IP: Parametri

Denominazione	Significato / Commento	Possibilità di selezione / campi dei valori
Name	Nome definibile liberamente per il servizio che viene utilizzato per l'identificazione nella definizione della regola o nel raggruppamento.	Immissione libera
Protocollo	Nome del tipo di protocollo:	TCP UDP Tutti
Porta sorgente	Viene eseguito un filtraggio in base al numero di porta qui indicato; esso definisce l'accesso al servizio nel mittente del telegramma.	Nella selezione del protocollo "Tutti" non è possibile una specificazione della porta. Esempi: *: La porta non viene controllata 20 o 21: FTP Service
Porta di destinazione	Viene eseguito un filtraggio in base al numero di porta qui indicato; esso definisce l'accesso al servizio nel destinatario del telegramma.	Nella selezione del protocollo "Tutti" non è possibile una specificazione della porta. Esempi: *: La porta non viene controllata 80: Web-HTTP-Service 102: Protocollo S7 - TCP/Port

4.3.8 definizione dei servizi ICMP

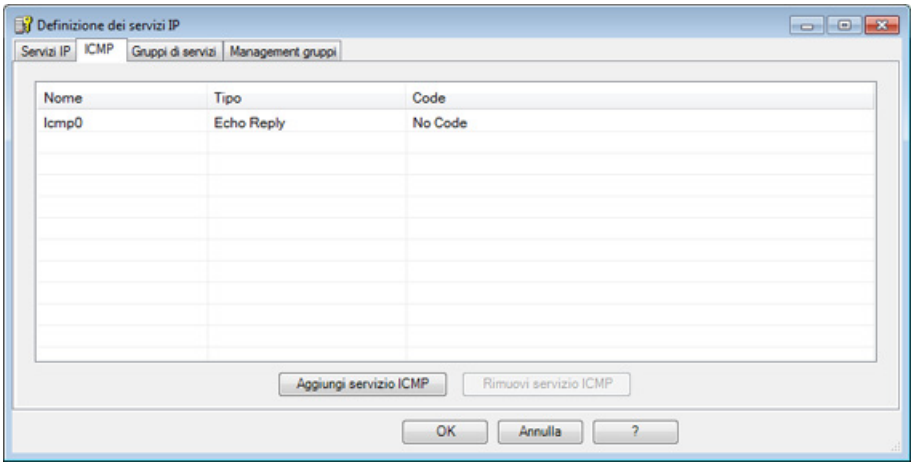
Con l'aiuto delle definizioni del servizio ICMP è possibile definire le regole del firewall che vengono utilizzate su determinati servizi ICMP. Per questo si assegna un nome e si assegnano al nome i parametri del servizio. I servizi definiti possono essere riuniti in gruppi con un nome di gruppo. Per la progettazione delle regola del filtro pacchetto utilizzare questo nome di gruppo.

A questa funzione si accede nel modo seguente

- Con la voce di menu "Opzioni " > "Servizi IP...", scheda "ICMP".

  o

- Dalla scheda "Regole IP" con il pulsante "Servizi IP...", scheda "ICMP"



Parametri per servizi ICMP

La definizione dei servizi ICMP viene eseguita con i seguenti parametri:

Tabella 4- 15 Servizi ICMP: Parametri

Denomina-zione	Significato / Commento	Possibilità di selezione / campi dei valori
Name	Nome definibile liberamente per il servizio che viene utilizzato per l'identificazione nella definizio-ne della regola o nel raggruppamento.	Immissione libera
Typ	Tipo del messaggio ICMP	Vedere la visualizzazione della finestra di dialogo.
Code	Codice del tipo ICMP	I valori sono in base al tipo selezionato.

4.3.9 Impostazione di regole del filtro pacchetto MAC

Con le regole del filtro pacchetto MAC è possibile filtrare i telegrammi MAC.

Nota

Nessuna regola MAC con la modalità Routing attivata

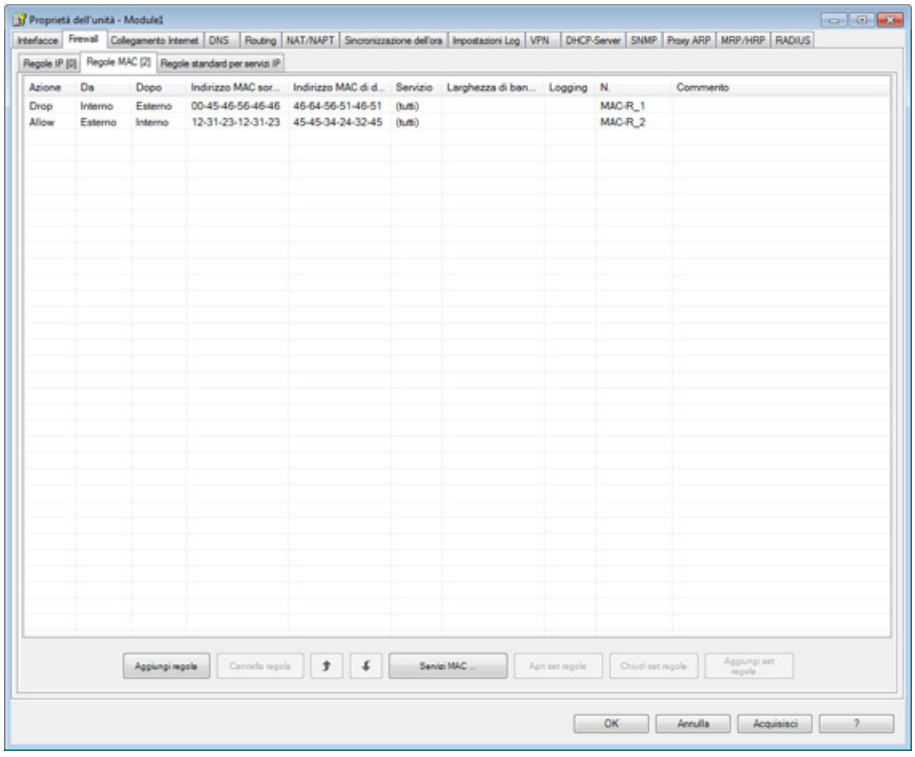
SCA. S

Se per l'unità SCALANCE S è stata attivata la modalità Routing, le regole MAC non vengono utilizzate.

Finestra di dialogo / scheda

Selezionare l'unità Security da modificare.

Per configurare il firewall selezionare la voce di menu "Modifica" > "Proprietà...", scheda "Firewall > "Regole MAC".



Inserimento delle regole del filtro pacchetto

Inserire in sequenza le regole del firewall nell'elenco; osservare la descrizione dei parametri e gli esempi nel seguente capitolo o nella guida in linea.

Utilizzo di set di regole firewall globali

I set di regole firewall globali assegnati all'unità Security vengono acquisiti automaticamente nell'elenco di regole locale. Se il set di regole assegnato alla fine dell'elenco di regole, esso viene modificato con la priorità più bassa. La priorità può essere modificata modificando la posizione nell'elenco delle regole.

La guida in linea descrive il significato dei singoli pulsanti.

4.3.10 Regole del filtro pacchetto MAC

L'elaborazione delle regole del filtro pacchetto MAC avviene in base alle seguenti analisi:

- Parametri inseriti nella regola;
- Priorità della regola all'interno del set di regole.

Regole del filtro pacchetto MAC

La progettazione di una regola MAC comprende i seguenti parametri:

Tabella 4- 16 Regole MAC: Parametri

Denominazione	Significato / Commento	Possibilità di selezione / campi dei valori
Azione	Definizione delle autorizzazioni (abilitazione/disabilitazione)	• Allow Autorizzazione di telegrammi in base alla definizione. • Drop Disabilitazione di telegrammi in base alla definizione. Per regole del collegamento create automaticamente: CP • Allow* • Drop* Se si selezionano queste regole, non ha luogo nessun livellamento con STEP 7. Le regole modificate non vengono quindi sovrascritte nell'SCT.
Da / A	Le direzioni di comunicazione ammesse.	Vengono descritte nella seguente tabella.
Indirizzo MAC sorgente	Indirizzo sorgente dei pacchetti MAC	In alternativa è possibile inserire nomi simbolici.
Indirizzo MAC di destinazione	Indirizzo di destinazione dei pacchetti MAC	
Servizio	Nome del servizio MAC o del gruppo di servizi utilizzato. "Any" raggruppa le direzioni ammesse per la singola voce.	La casella di riepilogo a discesa offre per la selezione i servizi progettati e i gruppi dei servizi. Nessuna indicazione significa: non viene controllato nessun servizio, la regola vale per tutti i servizi. **Avvertenza**: Per visualizzare i servizi MAC predefiniti nella casella di riepilogo, attivare prima questi servizi in modalità standard.

Denominazione	Significato / Commento	Possibilità di selezione / campi dei valori
Larghezza di banda (Mbit/s)	Possibilità di impostazione per una limitazione banda larga. Può essere inserita solo se selezionata nell'azione "Allow". Un pacchetto passa dal firewall, quando la regola di pass è giusta e la larghezza di banda ammessa per questa regola non è ancora stata superata.	CP x43-1 Adv. e SCALANCE S ≤ V3.0: 0.001 ... 100 CP 1628 e SCALANCE S ≥ V3.0: 0.001 ... 1000 Per le regole nei set di regole globali e personalizzati: 0.001 ... 100
Logging	Attivazione e disattivazione del logging per questa regola.	
N.	Numeri assegnati automaticamente per l'assegnazione ad una regola firewall progettata. Spostando le regole i numero vengono rilevati di nuovo.	
Commento	Spazio per la spiegazione della regola	Se un commento è contrassegnato con "AUTO", esso è stato creato per una regola di collegamento automatica.

Direzioni consentite

Possono essere impostate le seguenti direzioni:

Tabella 4- 17 Direzioni firewall CP

Possibilità di selezione / campi dei valori		Unità Security		Significato
Da	A	CP x43-1 Adv.	CP 1628	
Esterno	Stazione	x	x	Accesso da rete esterna a stazione.
Stazione	Esterno	x	x	Accesso dalla stazione alla rete esterna.
	Tunnel	x	x	Accesso dalla stazione al partner tunnel VPN.
Tunnel	Stazione	x	x	Accesso da partner tunnel VPN a stazione.

Tabella 4- 18 Direzioni firewall SCALANCE S

Possibilità di selezione / campi dei valori		Unità Security		
Da	A	S602	S61x	S623 / S627-2M
Interno	Esterno	x	x	x
	Tunnel	-	x	x
	Any	-	x	x
Esterno	Interno	x	x	x
	Any	-	-	x
	Tunnel	-	-	x

Possibilità di selezione / campi dei valori		Unità Security		
Tunnel	Interno	-	**x**	**x**
	Esterno	-	**x**	**x**
Any	Interno	-	**x**	**x**
	Esterno	-	-	**x**

Analisi delle regole attraverso l'unità Security

Le regole del pacchetto filtro vengono analizzate nel modo seguente:

- L'elenco viene analizzato dall'alto verso il basso; in caso di regole contrastanti vale la voce più in alto.
- Nelle regole per la comunicazione in direzione "Esterno" e dalla direzione "Esterno", per tutti i telegrammi rilevati in modo non esplicito vale: tutti i telegrammi sono disabilitati, eccetto i telegrammi autorizzati in modo esplicito nell'elenco.
- Nelle regole per la comunicazione in direzione "Tunnel" e dalla direzione "Tunnel", per tutti i telegrammi rilevati in modo non esplicito vale: tutti i telegrammi sono autorizzati, eccetto i telegrammi disabilitati in modo esplicito nell'elenco.

Nota

Regole IP applicate ai pacchetti IP, regole MAC applicate ai pacchetti Layer 2

Per il firewall possono essere definite sia regole IP, sia regole MAC. La modifica nel firewall è regolato in base al tipo Ethertype del pacchetto.

I pacchetti IP vengono inoltrato o bloccati in base alle regole IP mentre i pacchetti Layer 2 in base alle regole MAC.

Non è possibile filtrare un pacchetto IP utilizzando una regola firewall MAC, ad es. basato su un indirizzo MAC.

Esempi

L'esempio per il filtro pacchetto IP nel capitolo 5.4.3 (Pagina 145) può essere logicamente utilizzato sulle regole del filtro pacchetto MAC.

4.3.11 definizione dei servizi MAC

A questa funzione si accede nel modo seguente

- Con il comando di menu "Opzioni " > "Servizi MAC...".

  o

- Dalla scheda "Regole MAC" con il pulsante "Servizi MAC...".

Significato

Con l'aiuto delle definizioni del servizio MAC è possibile definire le regole del firewall che vengono utilizzate su determinati servizi. Si assegna un nome e si assegnano al nome i parametri del servizio. Inoltre è possibile riunire in gruppi i servizi definiti in un sottogruppo. Per la progettazione delle regole del filtro pacchetto globali o locali utilizzare questo nome.

Parametri per servizi MAC

Una definizione di servizio MAC contiene una categoria di parametri MAC specifici per il protocollo:

Tabella 4- 19 Parametri dei servizi MAC

Denominazione	Significato / Commento	Possibilità di selezione / campi dei valori
Name	Nome definibile liberamente per il servizio che viene utilizzato per l'identificazione nella definizione della regola o nel raggruppamento.	Immissione libera
Protocollo	Nome del tipo di protocollo: • ISO ISO contrassegna i telegrammi con le seguenti proprietà: Lengthfield <= 05DC (hex), DSAP= userdefined SSAP= userdefined CTRL= userdefined • SNAP SNAP contrassegna i telegrammi con le seguenti proprietà: Lengthfield <= 05DC (hex), DSAP=AA (hex), SSAP=AA (hex), CTRL=03 (hex), OUI=userdefined, OUI-Type=userdefined • PROFINET IO	• ISO • SNAP • PROFINET IO • 0x (immissione codice)
DSAP	Destination Service Access Point: Indirizzo destinatario LLC	
SSAP	Source Service Access Point: Indirizzo mittente LLC	
CTRL	LLC Control Field	
OUI	Organizationally Unique Identifier (i primi 3 byte dell'indirizzo MAC = identificazione costruttore)	
Tipo OUI	Tipo di protocollo/identificazione	
*) Le indicazioni del protocollo 0800 (hex) e 0806 (hex) non vengono accettate in quanto questi valori valgono per i telegrammi IP e ARP.		

Nota

Elaborazione per CP S7:

S7-CP

Vengono elaborate solo impostazioni relative ai frame ISO con DSAP=SSAP=FE (hex). Altri tipi di frame non sono rilevanti per i CP S7 e vengono quindi respinti dal firewall già prima dell'elaborazione.

Impostazioni specifiche per servizi SIMATIC NET

Per il filtraggio di servizi SIMATIC NET specifici utilizzare le seguenti impostazioni SNAP:

- DCP (Primary Setup Tool) :

  PROFINET IO

- SiCLOCK:

  OUI= 08 00 06 (hex) , OUI-Type= 01 00 (hex)

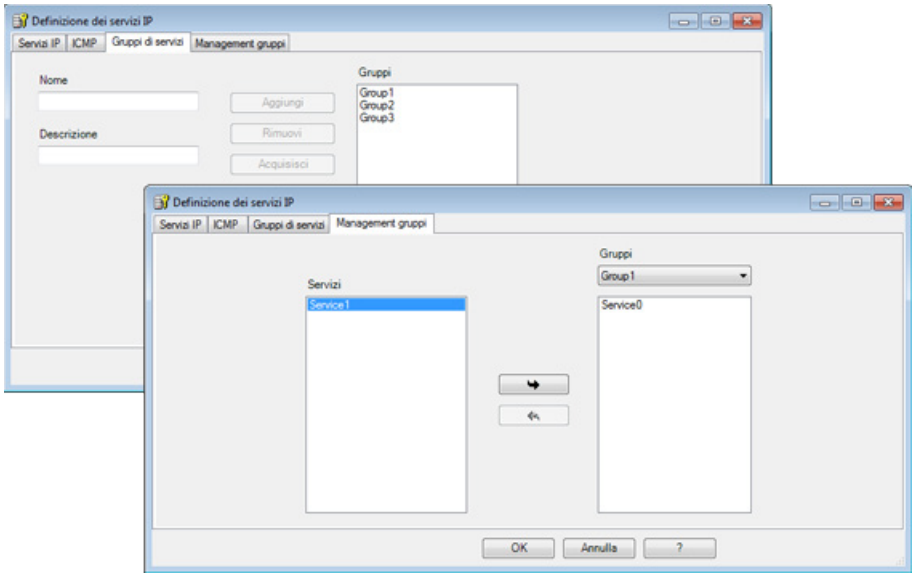
4.3.12 configurazione di gruppi di servizi

Formazioni di gruppi di servizi

È possibile riunire diversi servizi formando gruppi di servizi. In questo modo è possibile realizzare servizi complessi che possono essere utilizzati nelle regole del filtro pacchetti selezionando semplicemente il nome.

Finestre di dialogo / scheda

La finestra di dialogo si apre con la seguente voce di menu:
"Opzioni" > "Servizi IP..." o "Servizi MAC...", scheda "Gruppi di servizi".



4.3.13 Adattamento delle regole standard per servizi IP

S-V2.0 PC CP

A questa funzione si accede nel modo seguente:

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "Firewall" > scheda "Regole standard per servizi IP"

Significato delle impostazioni avanzate

Parametri	Significato in caso di attivazione
Utilizza opzioni di stato avanzate	Se si attiva questa casella di controllo, i collegamenti e gli stati del firewall vengono limitati per i nodi della rete. Le limitazioni sono: • max. 200 collegamenti in 5 secondi • max. 2000 stati firewall Se un nodo di rete supera una di queste limitazioni, il relativi indirizzo IP viene acquisito nella blacklist IP dell'unità Security. Il nodo non può più comunicare tramite l'unità Security. La blacklist IP dell'unità Security può essere osservata in modalità online.
Logging di tutte le regole attivate	Viene eseguito il logging dei pacchetti che vengono ammessi secondo le regole standard per i servizi IP.
Attiva test ICMP per interfacce	Le richieste ping in ingresso su un'interfaccia dell'unità Security possono essere inoltrate ad altre interfacce. In questo modo, dalla rete esterna possono ad es. essere eseguite richieste ping sull'interfaccia interna dell'unità Security.

Significato delle regole firmware standard

In questa finestra di dialogo esiste la possibilità di adattare le regole firewall specifiche per il servizio che sono impostate per l'impostazione dell'unità Security. Le impostazioni standard della finestra di dialogo corrispondono alle regole standard del firewall della relativa unità Security.

Regole firewall standard per SCALANCE S

Nella seguente tabella sono riportate le regole firewall standard per l'unità SCALANCE S. Le regole firewall sono in parte attive solo se il servizio interessato viene utilizzato dall'unità Security (ad es. SNMP).

Servizio	Direzione	Interfaccia X1 (rosso)	Interfaccia X2 (verde)	Interfaccia X3 (gialla) S62x	Interfaccia tunnel ~~S602~~
Routing interfaccia	in uscita	-	x	-	-
HTTPS		x	x*	x	x*
ICMP	in ingresso	-	x	-	x
ICMP Pathfinder S602 ≥V3.1	in uscita	-	x	-	-
SNMP	in ingresso	x	x	x	x
Syslog	in uscita	x	x	x	x
NTP	in uscita	x	x	x	x
DNS	in uscita	x	x	x	x
HTTP	in uscita	x	-	x	-
VPN (IKE)		x	-	x	-

Servizio	Direzione	Interfaccia X1 (rosso)	Interfaccia X2 (verde)	Interfaccia X3 (gialla) S62x	Interfaccia tunnel ~~S602~~
VPN (NAT Traversal)		x	-	x	-
BootP Server	in ingresso	-	x	x	-
BootP Client	in uscita	-	x	x	-
RADIUS	in uscita	x	x	x	x
CARP S62x ≥ V4.0	in uscita	x*	x*	-	-
Pfsync S62x ≥ V4.0	in uscita	-	-	x*	-

x attivato come standard

- disattivato come standard

* non adattabile

Regole firmware standard per CP S7

Nella seguente tabella sono riportate le regole firewall standard per i CP S7. Le regole firewall sono impostate solo se il servizio interessato è attivato nel Security Configuration Tool.

Servizio	Direzione	Esterno (GBit)	Interno (PN-IO)
VPN (IKE)		x*	-*
VPN (NAT Traversal)		x*	-*
BootP Server	in uscita	x*	x*
BootP Client	in ingresso	x*	x*

x attivato come standard

- disattivato come standard

* non adattabile

Entrambi i servizi "BootP Server" e "BootP Client" sono attivi insieme rispettivamente o sull'interfaccia esterna o sull'interfaccia interna. Sono attive o entrambe le regole firewall sull'interfaccia esterna o entrambe le regole firewall sull'interfaccia interna.

Progettazione di ulteriori proprietà dell'unità 5

5.1 Unità Security come router

5.1.1 Informazioni generali

Significato

Utilizzando l'unità Security come router, le reti sull'interfaccia interna, sull'interfaccia esterna e sull'interfaccia DMZ (solo SCALANCE S623/S627-2M, vedere sezione in basso) diventano sottoreti separate.

Esistono le seguenti possibilità:

- Routing - impostabile nella modalità standard e nella modalità estesa
- NAT/NAPT Routing - impostabile nella modalità estesa

Tutte le richieste ad una rete che non fanno parte di una sotto-rete vengono inoltrate in un'altra sotto-rete attraverso un router, vedere il seguente capitolo:

- Definizione del router standard e degli instradamenti (Pagina 164)

Attivare la modalità routing o l'interfaccia DMZ - scheda "Interfacce"

SCA. S

Se è stata attivata la modalità routing o l'interfaccia DMZ vengono inoltrati telegrammi destinati ad un indirizzo IP esistente nella rispettiva sotto-rete (interna, esterna, DMZ). Di conseguenza valgono le regole firewall progettate per la rispettiva direzione di trasmissione.

Per il modo di funzionamento è necessario progettare nella scheda "Interfacce" un indirizzo IP e una maschera di sottorete per l'interfaccia interna e/o per l'interfaccia DMZ per l'indirizzamento del router sulla sottorete interna e/o sulla sottorete DMZ. Tutte le richieste ad una rete che non fanno parte di una sotto-rete vengono inoltrate in un'altra sotto-rete attraverso il router standard.

Nota

Rispetto ad un funzionamento Bridge dell'unità Security, nella modalità Routing i tag VLAN vengono persi.

Modalità Bridge e Routing in SCALANCE S623/S627-2M

Nella rete DMZ si tratta di una sottorete separata. La differenza tra modalità Bridge e modalità Routing consiste nella suddivisione della rete esterna ed interna:

- Modo di funzionamento "Bridge": La rete interna ed esterna si trova nella stessa sottorete; la rete DMZ si trova nella sottorete separata.
- Modo di funzionamento "Routing": La rete interna la rete esterna si trovano rispettivamente in una propria sottorete; la rete DMZ si trova in un'ulteriore sottorete separata.

5.1.2 Definizione del router standard e degli instradamenti

A questa funzione si accede nel modo seguente

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "Routing"
3. Se si inserisce l'indirizzo IP / il FQDN per il router standard, tutti gli instradamenti vengono gestiti tramite questo router, se non è indicato nessun instradamento specifico. Gli instradamenti specifici possono essere inseriti nell'area di inserimento "Instradamenti".
4. Fare clic sul pulsante "Aggiungi instradamento".
5. Inserire i seguenti valori:

Parametri	Funzionamento	Valore di esempio
ID rete	Le richieste ai nodi delle sottoreti con l'ID di rete qui indicata e la maschera di sottorete indicata vengono inoltrate nella rete tramite l'indirizzo IP router indicato. in base all'ID di rete il router riconosce se un indirizzo di destinazione si trova nella sotto-rete o fuori dalla sotto-rete. L'ID di rete indicata non deve trovarsi nella stessa sottorete dell'indirizzo IP dell'interfaccia Security.	192.168.11.0
Finestra della sotto-rete	La maschera di sotto-rete struttura la rete. In base all'ID di rete e alla maschera di sottorete il router riconosce se un indirizzo di destinazione si trova all'intero o all'esterno della sottorete. La maschera della sottorete da indicare non può essere limitata ad un singolo nodo di rete (255.255.255.255).	255.255.255.0

Parametri	Funzionamento	Valore di esempio
Indirizzo IP router	Indirizzo IP / FQDN del router attraverso il quale si accede alla sottorete. L'indirizzo IP del router deve essere nella stessa sottorete dell'indirizzo IP dell'unità Security.	192.168.10.2 / myrouter.dyndns.org
Attiva rerouting (solo per unità SCALANCE S V3/V4)	Attivare questa casella opzione se i telegrammi dell'instradamento indicato devono essere in ingresso e in uscita sulla stessa interfaccia dell'unità Security (rerouting). Il rerouting è supportato solo sull'interfaccia interna dell'unità Security.	

Particolarità nel router standard

S≥V3.0

- Se nella scheda "Interfacce" l'assegnazione IP è configurata tramite "PPPoE", un router standard progettato viene ignorato in quanto l'instradamento standard porta automaticamente all'interfaccia PPPoE.
- Se nella scheda "Interfacce" l'assegnazione di indirizzo è configurata tramite "Indirizzo statico" e l'unità Security è collegata a Internet tramite un router DSL (NAPT), il router DSL deve essere inserito come router standard.
- Per le unità Security in modalità Ghost (solo SCALANCE S602 ≥ V3.1) non sono progettabili router standard in quanto essi vengono rilevati durante il tempo di esecuzione. Non sono progettabili instradamenti specifici per unità Security in modalità Ghost.

5.1.3 Routing NAT/NAPT

PC eP

Requisito richiesto

- Il progetto si trova in modalità estesa.
- L'unità Security si trova in modalità Routing o l'interfaccia DMZ (solo SCALANCE S623 / S627-2M) è attivata.

A questa funzione si accede nel modo seguente

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "NAT/NAPT"
3. A seconda dell'esigenza, attivare una conversione di indirizzo in base a NAT (Network Address Translation) o NAPT (Network Address Port Translation).

Conversione di indirizzo con NAT (Network Address Translation)

NAT è un protocollo per la conversione di indirizzi tra due aree di indirizzi.
La funzione principale è la conversione di indirizzi IP privati in indirizzi IP pubblici, ovvero in indirizzi IP che vengono utilizzati in Internet e anche instradati. In questo modo si ottiene che gli indirizzi IP della rete interna non vengono resi noti nella rete esterna. I nodi interni sono visibili nella rete esterna solo tramite l'indirizzo IP esterno definito nell'elenco di conversione indirizzi (tabella NAT). Se l'indirizzo IP esterno non è un indirizzo dell'unità Security e se l'indirizzo IP interno è univoco, esso viene indicato come 1:1 NAT. Con 1:1 NAT l'indirizzo interno senza conversione porta viene convertito sull'indirizzo esterno. In caso contrario si tratta di n:1 NAT.

Conversione di indirizzo con NAPT (Network Address Port Translation)

La conversione di indirizzi con NAPT modifica l'indirizzo IP di destinazione e la porta di destinazione in una relazione di comunicazione (inoltro della porta).

Vengono convertiti telegrammi provenienti dalla rete esterna o dalla rete DMZ e destinati all'indirizzo IP dell'unità Security. Se la porta di destinazione del telegramma è identica ad uno dei valori indicato nella colonna "Porta sorgente", l'unità Security sostituisce l'indirizzo IP di destinazione e la porta di destinazione come indicato nella riga corrispondente della tabella NAPT. In caso di risposta l'unità Security imposta come indirizzo IP sorgente e come porta sorgente i valori riportati nel telegramma iniziale come indirizzo IP di destinazione o porta di destinazione.

La differenza da NAT consiste nella possibilità di convertire anche le porte in questo protocollo. Non vi è nessuna conversione 1:1 dell'indirizzo IP. Inoltre esiste ancora solo un indirizzo IP pubblico che, con l'aggiunta di numero di porta viene convertito in una serie di indirizzi IP provati.

Conversione di indirizzi nei tunnel VPN

Le conversioni di indirizzi con NAT/NAPT possono essere eseguite anche per relazioni di comunicazione realizzate mediante tunnel VPN. Questa funzione viene supportata per i partner di collegamento del tipo SCALANCE M (solo 1:1-NAT) e SCALANCE S612 / S623 / S627-2M V4.

Ulteriori informazioni sulle conversioni di indirizzi nei tunnel VPN si trovano nei seguenti capitoli:

- Conversione di indirizzi NAT/NAPT (Pagina 168)
- Conversione di indirizzi con tunnel NAT/NAPT nei tunnel VPN (Pagina 174)

Conversione di regole NAT/NAPT da progetti precedenti

Con SCT V4.0 la modalità di progettazione delle regole NAT/NAPT e delle rispettive regole firewall è stata modificata. Se SCT V4.0 si vogliono adattare o estendere regole NAT/NAPT di un progetto creato con SCT V3.0/V3.1, è necessario dapprima convertire le regole NAT/NAPT in SCT V4.0. Selezionare quindi nel menu di scelta rapida di una regola NAT/NAPT la voce di menu "Converti tutte le regole NAT/NAPT in SCT V4" o "Converti regola NAT/NAPT selezionata in SCT V4". Per le regole NAT/NAPT convertite SCT genera quindi automaticamente regole firewall che abilitano la comunicazione nella direzione di conversione di indirizzi progettata. Modificare o rimuovere infine le regole firewall generate manualmente per le regole NAT/NAPT, se esse sono in contraddizione con le regole firewall generate automaticamente. Eseguire quindi gli adattamenti desiderati e/o le estensioni di regole NAT/NAPT e di regole firewall.

Controllo della coerenza - vanno osservate queste regole

Per ottenere registrazioni coerenti osservare inoltre le seguenti regole:

- L'indirizzo IP dell'interfaccia interna non deve essere utilizzata nella tabella NAT/NAPT.
- Un indirizzo IP, che viene utilizzato nell'elenco di conversione di indirizzi NAT/NAPT, non deve essere un indirizzo Multicast e un indirizzo Broadcast.
- Le porte esterne assegnate per la conversione NAPT si trova nel campo > 0 e ≤ 65535.

  Porta 123 (NTP), 443 (HTTPS), 514 (Syslog), 161 (SNMP), 67+68 (DHCP) und 500+4500 (IPsec) sono escluse se i rispettivi servizi sono attivati sull'unità Security.
- L'indirizzo IP esterno dell'unità Security o l'indirizzo IP dell'interfaccia DMZ può essere utilizzato nella tabella NAT solo per l'azione "Source-NAT".
- Controllo duplicato nella tabella NAT

  Un indirizzo IP esterno o un indirizzo IP nella rete DMZ, che viene utilizzato con direzione "Destination-NAT", "Source-NAT + Destination-NAT" o "Double-NAT" deve comparire una sola volta in ciascuna direzione indicata.
- Controllo duplicato nella tabella NAPT
  - Un numero di porta sorgente deve essere inserito una sola volta per ciascuna interfaccia.
  - I numeri di porta o le aree delle porte esterne e delle porte DMZ non devono sovrapporsi.
- Le porte NAPT interne possono trovarsi nel campo > 0 e ≤ 65535.

Dopo la conclusione delle immissioni eseguire un controllo della coerenza.

Selezionare quindi la voce di di menu "Opzioni > "Controlli di coerenza".

5.1.4 Conversione di indirizzi NAT/NAPT

Attivazione NAT

Il campo di immissione per NAT viene attivato. Le conversioni di indirizzi NAT vengono attivate solo con le voci descritte di seguito nell'elenco di conversione di indirizzi. Dopo la creazione di regole NAT le relative regole firewall vengono generate e visualizzate in modalità estesa, vedere capitolo:
Relazione tra router NAT/NAPT e firewall (Pagina 175)

Se per l'interfaccia esterna o l'interfaccia DMZ è attivato PPPoE, non è possibile progettare l'azione "Destination-NAT". Durante la progettazione dell'azione "Source-NAT" non è possibile inserire l'indirizzo IP nella casella di inserimento "Conversione sorgente" in quanto esso viene rilevato dinamicamente nel tempo di esecuzione.

Possibili azioni di conversione di indirizzi per NAT

Nelle seguenti tabelle sono illustrate le possibilità di inserimento per la conversione di indirizzi con NAT.

Azione "Destination-NAT" - "Redirect"

L'azione "Destination-NAT" può essere eseguita nella seguente direzione:

- Da esterno a interno

Se è attivata l'interfaccia DMZ dell'unità Security (solo SCALANCE S623/S627-2M), l'azione "Destination-NAT" può inoltre essere eseguita nelle seguenti direzioni:

- Da esterno a DMZ
- Da DMZ a interno
- Da DMZ a esterno

Se l'unità SCALANCE S si trova in un gruppo VPN (non per SCALANCE S602), l'azione "Destination-NAT" può inoltre essere eseguita nelle seguenti direzioni:

- Da tunnel a interno
- Da tunnel a esterno
- Da tunnel a DMZ (solo con l'interfaccia DMZ attivata)

Per la direzione "Da esterno a interno" vale ad esempio: Dell'indirizzo IP di destinazione di un telegramma proveniente dalla rete esterna ne viene controllata la corrispondenza con l'indirizzo IP indicato nella casella di inserimento "Indirizzo IP di destinazione". In caso di corrispondenza il telegramma viene inoltrato nella rete interna sostituendo l'indirizzo IPO di destinazione del telegramma con l'indirizzo IP indicato nella casella di inserimento "Conversione destinazione". È possibile l'accesso dall'esterno all'interno tramite l'indirizzo IP esterno.

La seguente tabella indica lo schema di inserimento per l'azione "Destination-NAT".

Casella	Inserimento possibile	Significato
Indirizzo IP sorgente	Irrilevante per questa azione.	-
Conversione sorgente	Irrilevante per questa azione.	-
Indirizzo IP di destinazione	Indirizzo IP nella rete sorgente	Indirizzo IP di destinazione nella rete sorgente con il quale si deve accedere ad un indirizzo IP nella rete di destinazione. L'indirizzo IP di destinazione non deve corrispondere all'indirizzo IP dell'unità Security nella rete sorgente. Se in un telegramma l'indirizzo IP di destinazione corrisponde all'indirizzo indicato, l'indirizzo viene sostituito con l'indirizzo IP corrispondente nella rete di destinazione. L'indirizzo IP di destinazione indicato diventa indirizzo Alias. Ciò significa che l'indirizzo IP indicato viene inoltre registrato come indirizzo IP sull'interfaccia selezionata. Gli indirizzi Alias vengono inoltre visualizzati nella scheda "Interfacce" dell'unità Security. Assicurarsi che con l'indirizzo Alias non vi sia nessun conflitto di indirizzo IP nella rete.
Conversione destinazione	Indirizzo IP nella rete di destinazione	L'indirizzo IP di destinazione viene sostituito dall'indirizzo IP qui indicato.
N.	-	Il numero progressivo assegnato da SCT che viene utilizzato per il riferimento alla regola firewall che viene generata da SCT per la regola NAT.

Azione "Source-NAT" - "Masquerading"

L'azione "Source-NAT" può essere eseguita nella seguente direzione:

- Da interno a esterno

Se è attivata l'interfaccia DMZ dell'unità Security (solo SCALANCE S623/S627-2M), l'azione "Source-NAT" può inoltre essere eseguita nelle seguenti direzioni:

- Da interno a DMZ
- Da esterno a DMZ
- Da DMZ a esterno

Se l'unità SCALANCE S si trova in un gruppo VPN (non per SCALANCE S602), l'azione "Source-NAT" può inoltre essere eseguita nelle seguenti direzioni:

- Da interno a tunnel
- Da esterno a tunnel
- Da DMZ a tunnel (solo con l'interfaccia DMZ attivata)

Per la direzione "Da interno a esterno" vale ad esempio: Dell'indirizzo IP sorgente di un telegramma proveniente dalla rete interna ne viene controllata la corrispondenza con l'indirizzo IP indicato nella casella di inserimento "Indirizzo IP sorgente". In caso di corrispondenza come nuovo indirizzo IP sorgente viene inoltrato nella´rete esterna il

telegramma con l'indirizzo IP esterno indicato nella casella di inserimento "Rilocazione della sorgente". Sulla rete esterna ha effetto l'indirizzo IP esterno.

La seguente tabella indica lo schema di inserimento per l'azione "Source-NAT".

Casella	Inserimento possibile	Significato
Indirizzo IP sorgente	Indirizzo IP nella rete sorgente	L'indirizzo IP sorgente del nodo interno indicato viene sostituito con l'indirizzo IP indicato nella casella di inserimento "Rilocazione della sorgente".
	Area di indirizzi IP/banda di indirizzi IP nella rete della sorgente	Gli indirizzi IP dell'area/della banda di indirizzi IP vengono sostituiti dall'indirizzo IP indicato nel campo di immissione "Conversione sorgente".
Conversione sorgente	Indirizzo IP nella rete di destinazione	Inserimento dell'indirizzo IP che deve essere utilizzato come nuovo indirizzo IP sorgente. Se l'indirizzo IP qui indicato non è un indirizzo IP dell'unità Security, esso diventa un indirizzo Alias. Ciò significa che l'indirizzo indicato viene inoltre registrato come indirizzo IP sull'interfaccia selezionata. Gli indirizzi Alias vengono inoltre visualizzati nella scheda "Interfacce" dell'unità Security. Assicurarsi che con l'indirizzo Alias non vi sia nessun conflitto di indirizzo IP nella rete.
Indirizzo IP di destinazione	Irrilevante per questa azione.	Irrilevante per questa azione.
Conversione destinazione	Irrilevante per questa azione.	Irrilevante per questa azione.
N.	-	Il numero progressivo assegnato da SCT che viene utilizzato per il riferimento alla regola firewall che viene generata da SCT per la regola NAT.

Nota

Per tutti i telegrammi che vanno da una rete sorgente a una rete di destinazione è possibile progettare una conversione di indirizzo in indirizzo IP dell'unità nella rete di destinazione. Inoltre dall'unità Security ad ogni telegramma viene assegnato un numero di porta. Si tratta di una conversione di indirizzo NAT n:1, nella quale diversi indirizzi IP della rete sorgente vengono convertiti in un indirizzo IP della rete sorgente.

Inserire ad esempio per la direzione "Da interno a esterno" i seguenti parametri:

- Azione: "Source-NAT"
- Da: "Interno"
- A "Esterno"
- Indirizzo IP sorgente: "*"
- Conversione sorgente: Indirizzo IP esterno dell'unità Security

Azione "Source-NAT + Destination-NAT" - "1:1-NAT"

L'azione "Source-NAT + Destination-NAT" può essere eseguita nella seguente direzione:

- Da interno a esterno

Se è attivata l'interfaccia DMZ dell'unità Security (solo SCALANCE S623/S627-2M), l'azione "Source-NAT + Destination-NAT" può inoltre essere eseguita nelle seguenti direzioni:

- Da interno a DMZ
- Da esterno a DMZ
- Da DMZ a esterno

Se l'unità SCALANCE S si trova in un gruppo VPN (non per SCALANCE S602), l'azione "Source-NAT + Destination-NAT" può inoltre essere eseguita nelle seguenti direzioni:

- Da esterno a tunnel
- Da interno a tunnel
- Da DMZ a tunnel (solo con l'interfaccia DMZ attivata)

Per la direzione "Da interno a esterno" vale ad esempio: Durante l'accesso da interno a esterno viene eseguita l'azione "Source-NAT". Durante l'accesso da esterno a interno viene eseguita l'azione "Destination-NAT".

La seguente tabella indica lo schema di inserimento per l'azione "Source-NAT + Destination-NAT":

Casella	Inserimento possibile	Significato
Indirizzo IP sorgente	Indirizzo IP nella rete sorgente	La progettazione viene sempre indicata nella direzione Source-NAT. Gli indirizzi IP della direzione Destination-NAT vengono quindi inseriti automaticamente da SCT.
	Area di indirizzi IP nella rete della sorgente	
Conversione sorgente	Indirizzo IP nella rete di destinazione	
Indirizzo IP di destinazione	Irrilevante per questa azione.	
Conversione destinazione	Irrilevante per questa azione.	
N.	-	Il numero progressivo assegnato da SCT che viene utilizzato per il riferimento alla regola firewall che viene generata da SCT per le regole NAT.

Azione "Double-NAT"

L'azione "Double-NAT" per le unità SCALANCE S può essere eseguita nelle seguenti direzioni:

- Da interno a esterno
- Da esterno a interno

Se è attivata l'interfaccia DMZ dell'unità Security (solo SCALANCE S623/S627-2M), l'azione "Double-NAT" può inoltre essere eseguita nelle seguenti direzioni:

- Da interno a DMZ
- Da esterno a DMZ
- Da DMZ a interno
- Da DMZ a esterno

In ciascuna direzione ha luogo sempre simultaneamente Source-NAT e Destination-NAT. Per la direzione "Da esterno a interno" vale ad esempio: Durante l'accesso da esterno a interno viene sostituito l'indirizzo IP sorgente del nodo esterno (Source-NAT). Inoltre l'accesso alla rete interna viene eseguito tramite l'indirizzo IP esterno indicato nella casella di inserimento "Indirizzo IP di destinazione" (Destination-NAT).

Questa azione può essere ad esempio eseguita se per un dispositivo, al quale si accede utilizzando Destination-NAT, è inserito un router standard diverso dall'unità Security. I telegrammi di risposta di questo dispositivo non vengono quindi inviati al router standard inserito, ma alla rispettiva interfaccia dell'unità Security.

La seguente tabella indica lo schema di inserimento per l'azione "Double-NAT":

Casella	Inserimento possibile	Significato
Indirizzo IP sorgente	Indirizzo IP nella rete sorgente	Indirizzo IP del nodo nella rete sorgente.
Conversione sorgente	-	La conversione di indirizzi Source-NAT viene eseguita sempre sull'indirizzo IP dell'unità Security nella rete di destinazione. Per questo motivo la casella di inserimento "Conversione sorgente" non è progettabile.
Indirizzo IP di destinazione	Indirizzo IP nella rete sorgente	Indirizzo IP di destinazione nella rete sorgente con il quale si deve accedere ad un indirizzo IP nella rete di destinazione. Se in un telegramma l'indirizzo IP di destinazione corrisponde all'indirizzo IP indicato, l'indirizzo IP viene sostituito con l'indirizzo IP indicato nella casella di inserimento "Conversione destinazione". Se l'indirizzo IP qui indicato non è un indirizzo IP dell'unità Security, esso diventa un indirizzo Alias. Ciò significa che l'indirizzo indicato viene inoltre registrato come indirizzo IP sull'interfaccia selezionata. Gli indirizzi Alias vengono inoltre visualizzati nella scheda "Interfacce" dell'unità Security. Assicurarsi che con l'indirizzo Alias non vi sia nessun conflitto di indirizzo IP nella rete.
Conversione destinazione	Indirizzo IP nella rete di destinazione	L'indirizzo IP di destinazione viene sostituito dall'indirizzo IP qui indicato.
N.	-	Il numero progressivo assegnato da SCT che viene utilizzato per il riferimento alla regola firewall che viene generata da SCT per la regola NAT.

Attivazione NAPT

Il campo di immissione per NAPT viene attivato. Le conversioni NAPT vengono attivate nell'elenco solo con le voci descritte di seguito. Dopo la creazione di regole NAPT le relative regole firewall vengono generate e visualizzate in modalità estesa, vedere capitolo: Relazione tra router NAT/NAPT e firewall (Pagina 175)

La conversione di indirizzi IP con NAPT può essere eseguita nella seguente direzione:

- Da esterno a interno

Se è attivata l'interfaccia DMZ dell'unità Security (solo SCALANCE S623/S627-2M), la conversione di indirizzi IP con NATP può inoltre essere eseguita nelle seguenti direzioni:

- Da esterno a DMZ
- Da DMZ a interno
- Da DMZ a esterno

Se l'unità SCALANCE S si trova in un gruppo VPN (non per SCALANCE S602), la conversione di indirizzi IP con NAPT può inoltre essere eseguita nelle seguenti direzioni:

- Da esterno a tunnel
- Da tunnel a interno
- Da tunnel a esterno
- Da DMZ a tunnel (solo con l'interfaccia DMZ attivata)
- Da tunnel a DMZ (solo con l'interfaccia DMZ attivata)

Per la direzione "Da esterno a interno" vale ad esempio: I telegrammi destinati all'indirizzo IP esterno dell'unità Security e alla porta inserita nella colonna "Porta sorgente" vengono inoltrati all'indirizzo IP di destinazione della rete interna e alla porta di destinazione indicata.

La seguente tabella indica lo schema di inserimento per la conversione di indirizzi con NAPT:

Casella	Inserimento possibile	Significato
Porta sorgente	Porta TCP/UDP o area della porta Esempio di inserimento di un'area della porta: 78:99	Un nodo nella rete sorgente può inviare un telegramma ad un nodo nella rete di destinazione utilizzando questo numero di porta.
Indirizzo IP di destinazione	Indirizzo IP nella rete di destinazione	I telegrammi destinati all'indirizzo IP dell'unità Security nella rete sorgente e alla porta TCP/UDP indicata nella casella "Porta sorgente" vengono inoltrati all'indirizzo IP indicato.
Porta di destinazione	Porta TCP/UDP	Numeri di porta ai quali vengono inoltrati telegrammi provenienti dalla rete sorgente.
Protocollo	• TCP+UDP • TCP • UDP	Selezione della famiglia di protocolli per i numeri di porta indicati
N.	-	Il numero progressivo assegnato da SCT che viene utilizzato per il riferimento alla regola firewall che viene generata da SCT per la regola NAPT.

Vedere anche

Regole del filtro pacchetto IP (Pagina 145)

5.1.5 Conversione di indirizzi con tunnel NAT/NAPT nei tunnel VPN

Significato

Le conversioni di indirizzi con NAT/NAPT possono essere eseguite anche per relazioni di comunicazione realizzate mediante tunnel VPN.

Requisiti richiesti

Per un'unità SCALANCE S che deve eseguire una conversione di indirizzi con NAT/NAPT in un tunnel VPN valgono in generale i seguenti requisiti:

- L'unità SCALANCE S si trova in un gruppo VPN.
- L'unità SCALANCE S si trova in modalità Routing e/o l'interfaccia DMZ dell'unità SCALANCE S è attivata.
- L'interfaccia tunnel è attivata.

Direzioni di conversione di indirizzi supportate

Vengono supportate le direzioni di conversione di indirizzi descritte nel seguente capitolo:
Conversione di indirizzi NAT/NAPT (Pagina 168)

Azioni di conversione di indirizzi supportate

In caso di relazioni di comunicazione via tunnel vengono supportate le seguenti azioni di conversione di indirizzi:

- Destination-NAT ("Redirect")
- Source-NAT ("Masquerading")
- Source-NAT e Destination-NAT ("1:1-NAT")
- NAPT ("Portforwarding")

Informazioni fondamentali sulle azioni di conversione di indirizzi si trovano nel seguente capitolo:
Conversione di indirizzi NAT/NAPT (Pagina 168)

Accoppiamenti VPN supportati

In combinazione con NAT/NAPT vengono supportati i seguenti accoppiamenti VPN:

Accoppiamento VPN		Il collegamento VPN viene inizializzato da	La conversione di indirizzi viene eseguita da
SCALANCE S (a)	SCALANCE S (b)	SCALANCE S (a) o SCALANCE S (b)	SCALANCE S (a) e/o SCALANCE S (b)
SCALANCE S	CP S7 / CP PC	SCALANCE S o CP S7 / CP PC	SCALANCE S
SCALANCE S	SCALANCE M	SCALANCE M	SCALANCE S e/o SCALANCE M*
SOFTNET Security Client	SCALANCE S	SOFTNET Security Client	SCALANCE S
SCALANCE S	NCP VPN Client (Android)	NCP VPN Client (Android)	SCALANCE S

* Viene supportato solo 1:1-NAT.

Le unità SCALANCE S del tipo SCALANCE S623 V4 e SCALANCE S627-2M V4, che dispongono di un punto terminale VPN su un'interfaccia esterna e sull'interfaccia DMZ possono eseguire conversioni di indirizzi simultanee su entrambe le interfacce.

Comportamento di conversione di indirizzi in caso di partecipazione a più gruppi VPN

Se un'unità SCALANCE S è un nodo di diversi gruppi VPN, per tutti i collegamenti VPN di questa unità SCALANCE S valgono le regole di conversione di indirizzi progettate per l'interfaccia tunnel dell'unità SCALANCE S.

Osservare quanto segue:

Non appena è stata configurata una conversione di indirizzo NAT nella o dalla direzione tunnel, gli indirizzi IP interessati delle regole di conversione di indirizzi NAT sono ancora raggiungibili tramite il VPN.

5.1.6 Relazione tra router NAT/NAPT e firewall

Significato

Dopo la creazione di regole NAT/NAPT, l'SCT genera automaticamente regole firewall che abilitano la comunicazione nella direzione di conversione di indirizzi progettata. Le regole firewall possono eventualmente essere spostate ed estese (indirizzi IP supplementari / area di indirizzi IP / banda di indirizzi IP, servizi, larghezza di banda). Inoltre le regole firewall generate automaticamente devono essere controllate in base alla loro priorità in funzione della posizione. Se nell'elenco delle regole si trovano anche regole firewall progettate manualmente e con priorità superiore a quella delle regole firewall generate automaticamente, eventualmente non vengono eseguiti NAT/NAPT.

I parametri firewall generali da SCT non possono essere adattati. Dopo la disattivazione di NAT/NAPT vengono cancellate le regole firewall generate da SCT.

Per il semplice riferimento tra regole NAT/NAPT e le regole rispettive firewall, le regole nelle schede "NAT/NAPT" e "Firewall" sono contrassegnate con numeri progressivi corrispondenti.

Nella tabella seguente sono riportati gli schemi delle regole firewall che vengono generate per le unità SCALANCE S per le regole NAT.

Tabella 5- 1 Conversione dell'indirizzo NAT e relative regole firewall per le unità SCALANCE S

Azione NAT	**Regola firewall creata**				
	Azione	**Da**	**A**	**Indirizzo IP sorgente**	**Indirizzo IP di destinazione**
Destination-NAT	Allow	Rete sorgente	Rete di destinazione	-	Indirizzo IP che è stato indicato nel campo di immissione "Indirizzo IP di destinazione"
NAT sorgente	Allow	Rete sorgente	Rete di destinazione	Indirizzo IP del nodo che è stato indicato nella casella di inserimento "Indirizzo IP sorgente"	-
Source-NAT + Destination-NAT	Allow	Rete sorgente	Rete di destinazione	Indirizzo IP del nodo che è stato indicato nella casella di inserimento "Indirizzo IP sorgente"	-
	Allow	Rete di destinazione	Rete sorgente	-	Indirizzo IP del nodo inserito da SCT nel campo di immissione "Indirizzo IP di destinazione"
Double-NAT	Allow	Rete sorgente	Rete di destinazione	Indirizzo IP del nodo che è stato indicato nella casella di inserimento "Indirizzo IP sorgente"	Indirizzo IP che è stato indicato nel campo di immissione "Indirizzo IP di destinazione"
	Allow	Rete sorgente	Rete di destinazione	Indirizzo IP del nodo che è stato indicato nella casella di inserimento "Indirizzo IP sorgente"	Indirizzo IP del nodo che è stato indicato nella casella di inserimento "Conversione destinazione"

Nella tabella seguente sono riportati gli schemi delle regole firewall che vengono generate per il CP x43-1 Adv. per le regole NAT.

Tabella 5- 2 Conversione dell'indirizzo NAT e relative regole firewall per il CP x43-1 Adv.

Azione NAT	**Regola firewall creata**				
	Azione	**Da**	**A**	**Indirizzo IP sorgente**	**Indirizzo IP di destinazione**
Destination-NAT	Drop	Esterno	Stazione	-	-
	Allow	Esterno	Any	-	Indirizzo IP del nodo che è stato indicato nella casella di inserimento "Conversione destinazione"
NAT sorgente	Allow	Any	Esterno	Indirizzo IP che è stato indicato nel campo di immissione "Conversione sorgente"	-
Source-NAT + Destination-NAT	Allow	Any	Esterno	Indirizzo IP che è stato indicato nel campo di immissione "Conversione sorgente"	-
	Drop	Esterno	Stazione	-	-
	Allow	Esterno	Any	-	Indirizzo IP del nodo che è stato indicato nella casella di inserimento "Conversione destinazione"

Nella tabella seguente è riportato lo schema delle regole firewall generate per le unità SCALANCE S per le regole NAPT.

Tabella 5- 3 Conversioni NAPT e regole firewall create per le unità SCALANCE S

Regola firewall creata					
Azione	**Da**	**A**	**Indirizzo IP sorgente**	**Indirizzo IP di destinazione**	**Servizio**
Allow	Rete sorgente	Rete di destinazione	-	Indirizzo IP dell'unità Security nella rete sorgente.	[Servizio_regola NAPT]

Nella tabella seguente è riportato lo schemi delle regole firewall che vengono generate per il CP x43-1 Adv. per le regole NAPT.

Tabella 5- 4 Conversioni NAPT e regole firewall create per il CP x43-1 Adv.

Regole firewall create					
Azione	**Da**	**A**	**Indirizzo IP sorgente**	**Indirizzo IP di destinazione**	**Servizio**
Drop	Esterno	Stazione	-	-	[Servizio_regola NAPT]
Allow	Esterno	Any	-	Indirizzo IP del nodo che è stato indicato nella casella di inserimento "Indirizzo IP di destinazione"	[Servizio_regola NAPT]

Stateful Packet Inspection

Firewall e router NAT/NAPT supportano il dispositivo "Stateful Packet Inspection". Di conseguenza i telegrammi di risposta possono attraversare il router NAT/NAPT e il firewall, senza che i relativi indirizzi debbano essere ulteriormente acquisiti nella regola firewall e nella conversione di indirizzo NAT/NAPT.

5.1.7 Relazione tra router NAT/NAPT e firewall specifico per l'utente

Significato

Dopo la creazione di regole NAT/NAPT, l'SCT genera automaticamente nel firewall specifico per l'utente un set di regole IP personalizzato abilita la comunicazione nella direzione di conversione di indirizzi progettata. A questo set di regole IP personalizzato è quindi possibile assegnare singoli o più utenti e/o singoli o più ruoli (solo per unità SCALANCE S a partire da V4).

Le regole firewall possono eventualmente essere spostate ed estese (indirizzo IP supplementare, servizi, larghezza di banda). I parametri firewall generali da SCT non possono essere adattati. Se un set di regole IP personalizzato viene trascinato su un'unità Security con NAT/NAPT disattivato per Drag and Drop, anche le regole NAT/NAPT del firewall specifico per l'utente non possono essere utilizzate su questa unità Security.

Nota

L'operazione di conversione degli indirizzi "Double-NAT" non viene supportata in relazione al firewall specifico per l'utente.

A questa funzione si accede nel modo seguente

Scheda "NAT" o "NAPT" nella finestra di dialogo della configurazione per set di regole IP personalizzati, vedere il seguente capitolo:
Set di regole IP specifiche per l'utente (Pagina 138)

Direzioni di conversione di indirizzi supportate per l'azione "Source-NAT"

L'azione "Source-NAT" può essere eseguita nelle seguenti direzioni:

- Da esterno a DMZ
- Da DMZ a esterno

Nella casella "Indirizzo IP sorgente" non può essere inserito nessun indirizzo IP. Esso viene inserito automaticamente durante il login del nodo all'unità Security.

Direzioni di conversione di indirizzi supportate per l'azione "Destination-NAT"

L'azione "Destination-NAT" può essere eseguita nelle seguenti direzioni:

- Da esterno a interno
- Da esterno a DMZ
- Da DMZ a interno
- Da DMZ a esterno
- Tunnel verso l'interno (solo SCALANCE S612/S623/S627-2M a partire da V4)
- Tunnel verso l'esterno (solo SCALANCE S612/S623/S627-2M a partire da V4)
- Tunnel verso DMZ (solo SCALANCE S612/S623/S627-2M a partire da V4)

Direzioni di conversione di indirizzi supportate per l'azione "Source-NAT + Destination-NAT"

L'azione "Source-NAT + Destination-NAT" può essere eseguita nelle seguenti direzioni:

- Da esterno a DMZ
- Da DMZ a esterno

Nella casella "Indirizzo IP sorgente" non può essere inserito nessun indirizzo IP. Esso viene inserito automaticamente durante il login del nodo all'unità Security.

Direzioni di conversione di indirizzi supportati per NAPT

La conversione di indirizzi con NAPT può essere eseguita nelle seguenti direzioni:

- Da esterno a interno
- Da esterno a DMZ
- Da DMZ a interno
- Da DMZ a esterno
- Tunnel verso l'interno (solo SCALANCE S612/S623/S627-2M a partire da V4)

- Tunnel verso l'esterno (solo SCALANCE S612/S623/S627-2M a partire da V4)
- Tunnel verso DMZ (solo SCALANCE S612/S623/S627-2M a partire da V4)

Conversione di indirizzi NAT/NAPT e relativi set di regole IP personalizzati

Nelle regole firewall per set di regole IP personalizzati, generati sulla base di regole NAT/NAPT, nella casella "Indirizzo IP sorgente" non può essere inserito l'indirizzo IP. Esso viene inserito automaticamente durante il login del nodo nel modulo Security. Le restanti proprietà sono identiche alle regole firewall generate localmente per i singoli moduli Security.
Vedere capitolo:
Relazione tra router NAT/NAPT e firewall (Pagina 175)

5.2 Unità Security come server DHCP

5.2.1 Informazioni generali

SCA. S

Informazioni generali

L'unità Security può essere utilizzata sulla rete interna e sulla rete DMZ come server DHCP (DHCP = Dynamic Host Configuration Protocoll). In questo modo è possibile assegnare automaticamente gli indirizzi IP agli apparecchi collegati.

È possibile il funzionamento simultaneo di server DHCP su entrambe le interfacce. S62x

Gli indirizzi IP vengono ripartiti dinamicamente da una banda di indirizzi indicata oppure viene assegnato un determinato indirizzo IP di un determinato dispositivo. Per consentire che i dispositivi sull'interfaccia interna o sull'interfaccia DMZ ricevano sempre lo stesso indirizzo IP per la configurazione firewall, l'assegnazione di indirizzi può essere solo statica in base all'indirizzo MAC e in base all'ID client.

Requisito richiesto

Nella rete interna o nella rete DMZ l'apparecchio deve essere configurato in modo che esso rilevi l'indirizzo IP da un server DHCP.

A seconda del modo di funzionamento, l'unità Security trasmette ai nodi nella rispettiva sotto-rete un indirizzo IP del router standard oppure è necessario comunicare ai nodi nella sotto-rete un indirizzo IP router.

- L'indirizzo IP del router viene trasmesso

  Nei seguenti casi dal protocollo DHCP dell'unità Security viene trasmesso ai nodi un indirizzo IP del router:

  – Il nodo si trova sull'interfaccia DMZ (solo SCALANCE S623/S627-2M)
    L'unità Security trasmette in questo caso il proprio indirizzo IP come indirizzo IP del router.

  – Il nodo si trova sull'interfaccia interna e l'unità Security è configurata per il funzionamento router
    L'unità Security trasmette in questo caso il proprio indirizzo IP come indirizzo IP del router.

  – Il nodo si trova sull'interfaccia interna e l'unità Security non è configurata per il funzionamento router, ma nella configurazione dell'unità Security è indicato un router standard.
    L'unità Security trasmette in questo caso l'indirizzo IP del router standard come indirizzo IP del router.

- L'indirizzo IP del router non viene trasmesso

  Nei seguenti casi inserire manualmente l'indirizzo IP router nel nodo:

  – Il nodo si trova sull'interfaccia interna e l'unità Security non è configurata per il funzionamento router. Inoltre nella configurazione dell'unità Security non è indicato nessun router standard.

Vedere anche

Controlli di coerenza (Pagina 61)

5.2.2 Configurazione del server DHCP

Requisito richiesto

La scheda "Server DHCP" viene visualizzata solo se il progetto si trova in modalità estesa.

Nota

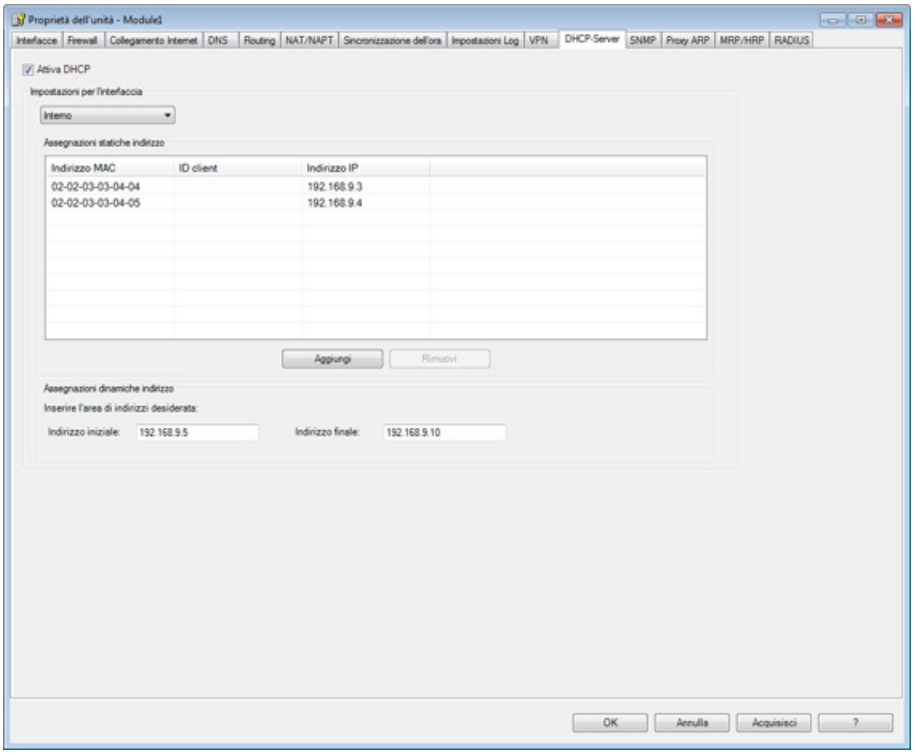
Non è possibile una ricommutazione alla modalità standard

Non appena è stata modificata la configurazione per il progetto attuale, non è più possibile annullare una commutazione nella modalità estesa precedentemente eseguita.

Rimedio SCT Standalone: chiudere il progetto senza salvarlo e aprirlo di nuovo.

A questa funzione si accede nel modo seguente

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "Server DHCP".



3. Attivare la casella di controllo "Attiva DHCP".
4. Selezionare per quale interfaccia devono essere eseguite le impostazioni DHCP.
5. Eseguire l'assegnazione di indirizzi. Per la configurazione esistono le due seguenti possibilità:

- Assegnazioni statiche di indirizzo

  Agli apparecchi con un determinato indirizzo MAC o ID client vengono assegnati rispettivamente indirizzi IP preimpostati. Inserire quindi questi apparecchi nell'elenco di indirizzi nel campo di immissione "Assegnazione di indirizzi statica". Questa opzione è opportuna in caso di regole firewall con indicazione esplicita di indirizzo sorgente o indirizzo IP di destinazione.

- Assegnazioni dinamiche di indirizzo

  I dispositivi il cui indirizzo MAC o ID client non sono stati indicati in modo esplicito ottengono un indirizzo IP qualsiasi dalla banda di indirizzi indicata. Questa banda di indirizzi si imposta nel campo di immissione "Assegnazione di indirizzi dinamica".

Nota

Assegnazione dinamica dell'indirizzo - Comportamento dopo l'interruzione della tensione di alimentazione

Fare attenzione che gli indirizzi IP assegnati dinamicamente non vengono salvati se la tensione di alimentazione viene interrotta. Al ripristino della tensione di alimentazione i nodi devono richiedere di nuovo un indirizzo IP.

Di conseguenza è necessario prevedere l'assegnazione dinamica di indirizzo solo per i seguenti nodi:

- nodi che vengono usati temporalmente nella sotto-rete (come per esempio apparecchi di service);
- nodi che trasmettono al server DHCP un indirizzo IP assegnato una volta come "indirizzo primario" ad una nuova richiesta (come per esempio stazioni PC).

Per i nodi in esercizio permanente l'assegnazione statica dell'indirizzo deve essere eseguita tramite indicazione di un'ID client (raccomandata per CP S7 a causa della sostituzione semplice dell'unità) o dell'indirizzo MAC.

Sono supportati i nomi simbolici

Nella funzione qui descritta è possibile inserire indirizzi IP o MAC anche come nomi simbolici.

Controllo della coerenza - vanno osservate queste regole

Per l'inserimento rispettare le regole riportate qui di seguito:

- Gli indirizzi IP assegnati nell'elenco di indirizzi nel campo di immissione "Assegnazioni statiche di indirizzo" non devono trovarsi nel campo degli indirizzi IP dinamici.
- I nomi simbolici devono disporre di un'assegnazione di indirizzo numerica. Se si reinserisce un nome simbolico è necessario eseguire ancora l'assegnazione di indirizzo nella finestra di dialogo "Nome simbolico".
- Gli indirizzi IP, gli indirizzi MAC e le ID client devono esistere una sola volta nell'area di inserimento "Assegnazioni statiche di indirizzo" (riferiti all'unità Security).
- Per gli indirizzi IP assegnati staticamente è necessario inserire l'indirizzo MAC o l'ID client (nome computer).
- L'ID client è una stringa di caratteri con max. 63 caratteri. Posso essere utilizzati solo i seguenti caratteri: a-z, A-Z, 0-9 e - (trattino).

  Avvertenza

  In SIMATIC S7 agli apparecchi sull'interfaccia Ethernet può essere assegnata un'ID client tramite DHCP per il riferimento ad un indirizzo IP.

  Nei PC il procedimento dipende dal sistema operativo utilizzato; per l'assegnazione si raccomanda di utilizzare l'indirizzo MAC.
- Per gli indirizzi IP assegnati staticamente è necessario indicare l'indirizzo IP.

- I seguenti indirizzi IP non devono trovarsi nell'area delle assegnazioni dinamiche di indirizzo:
  - tutti gli indirizzi IP router nella scheda "Routing"
  - Syslog server
  - Router standard
  - Indirizzo(i) dell'unità Security.
- L'unità Security supporta DHCP sull'interfaccia verso la sottorete interna e sull'interfaccia verso la rete DMZ. Da questo comportamento di esercizio dell'unità Security risultano inoltre i seguenti requisiti per gli indirizzi IP nell'area delle assegnazioni dinamiche di indirizzo:
  - modalità bridge

    L'area deve trovarsi nella rete definita dall'unità Security.
  - Modalità Routing

    L'area deve trovarsi nella rete interna definita dall'unità Security.

    Avvertenza

    La rete DMZ rappresenta già una sottorete separata. In caso di utilizzo di DHCP sull'interfaccia DMZ è necessario osservare che l'area di indirizzo IP libera (indirizzi IP dinamici) si trovi all'interno della sottorete DMZ.
- L'area di indirizzi IP libera deve essere indicata completamente inserendo l'indirizzo iniziale e l'indirizzo finale. L'indirizzo finale deve essere maggiore dell'indirizzo iniziale.
- Gli indirizzi IP che si inseriscono nell'elenco di indirizzi nel campo di immissione "Assegnazione statica di indirizzo" devono trovarsi nel campo di indirizzi della sottorete interna o nella rete DMZ dell'unità Security.

Osservare le descrizioni nel capitolo Controlli di coerenza (Pagina 61).

5.3 Sincronizzazione dell'ora

5.3.1 Informazioni generali

Significato

Per il controllo della validità dell'ora di un certificato e per il timbro dell'ora di registrazioni log, sull'unità Security viene indicata la data e l'ora.

Sono progettabili le seguenti alternative:

- Posizioni automatiche dell'ora dell'unità con l'ora del PC durante il caricamento di una configurazione. SCA. S
- Posizioni automatiche e sincronizzazione periodica dell'ora tramite un server Network Time Protocol (server NTP).

Nota

Prima che le funzioni Security di un CP vengano utilizzate, esse devono ricevere un telegramma di sincronizzazione dell'ora valido dal master dell'ora.

Sincronizzazione con un server NTP

Per la creazione del server NTP valgono le seguenti regole:

- I server NTP possono essere creati per tutto il progetto tramite il menu SCT "Opzioni" > "Configurazione del server NTP...". Assegnare un server NTP ad un'unità Security tramite la scheda delle proprietà "Sincronizzazione dell'ora". Se diverse unità Security utilizzano lo stesso server NTP nel progetto SCT, i loro dati devono essere inseriti solo una volta.
- Per tutto il progetto possono essere creati 32 server NTP.
- Ad un'unità Security possono essere assegnati max. 4 server NTP.
- I nomi simbolici vengono supportati durante la definizione dei server NTP.
- FQDN vengono vengono supportati durante la definizione dei server NTP.
- I server NTP già creati STEP 7 migrano l'indirizzo IP e l'intervallo di aggiornamento in SCT. CP
- In caso di selezione di "Sincronizzazione dell'ora con NTP (protetta)", l'unità Security accetta solo l'ora di server NTP protetti, configurati in modo corrispondente. Non è possibile una configurazione combinata di server NTP non protetti e protetti su un'unità Security.

5.3.2 Configurazione della gestione dell'ora

A questa funzione si accede nel modo seguente

Voce di menu SCT:

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "Sincronizzazione dell'ora"

Voce di menu STEP 7 (se l'opzione "Attiva sincronizzazione dell'ora nel metodo NTP" è attivata): "Sincronizzazione dell'ora" > "Attiva configurazione NTP estesa", pulsante "Esegui".

In alternativa alla sincronizzazione dell'ora

Sono progettabili le seguenti alternative:

Tabella 5- 5 Sincronizzazione dell'ora per CP

Possibilità di selezione	Significato / Effetto
Nessuna sincronizzazione dell'ora	Nessuna sincronizzazione dell'ora tramite il PC PC o un server NTP.
Sincronizzazione dell'ora con NTP	Posizioni automatiche e sincronizzazione periodica dell'ora tramite un server NTP.
Sincronizzazione dell'ora con NTP (protetta)	Posizioni automatiche e sincronizzazione periodica dell'ora tramite un server NTP (protetto).

Tabella 5- 6 Sincronizzazione dell'ora per SCALANCE S ≥ V3.0

Possibilità di selezione	Significato / Effetto
Nessuna sincronizzazione dell'ora	Nessuna sincronizzazione dell'ora.
Imposta ora per ciascun caricamento	Posizioni automatiche dell'ora dell'unità con l'ora del PC durante il caricamento di una configurazione.
Sincronizzazione dell'ora con NTP	Posizioni automatiche dell'ora tramite un server NTP.
Sincronizzazione dell'ora con NTP (protetta) S≥V4.0	Posizioni automatiche e sincronizzazione periodica dell'ora tramite un server NTP (protetto).

Selezione della modalità per la sincronizzazione dell'ora

Procedere nel modo seguente:

1. Selezionare la modalità di sincronizzazione.
2. Per SCALANCE S < V3.0: In caso di sincronizzazione attraverso un server NTP inserire l'intervallo di aggiornamento in secondi. Per SCALANCE S ≥ V3.0 viene inoltre definito automaticamente un intervallo di tempo per l'interrogazione del server NTP.

   Nota

   CP

   I server NTP creati in STEP 7 vengono migrati automaticamente in SCT con l'intervallo di aggiornamento. L'intervallo di aggiornamento può essere modificato solo in STEP 7.

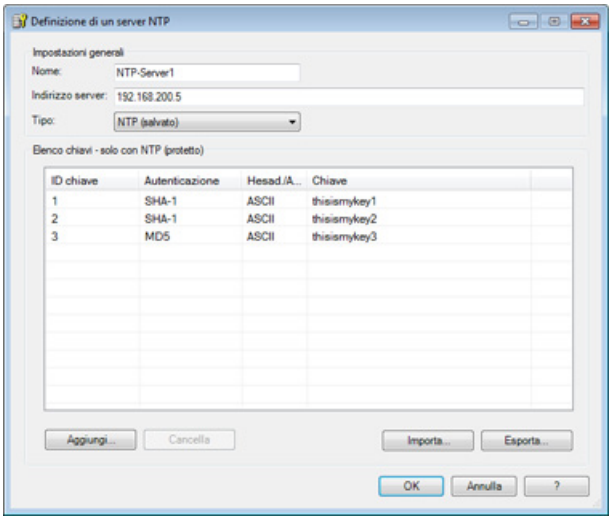
3. Se è stata selezionata la modalità di sincronizzazione "Sincronizzazione dell'ora con NTP" o "Sincronizzazione dell'ora con NTP (protetta)", con il pulsante "Aggiungi" assegnare all'unità Security un server NTP già creato dello stesso tipo selezionato nella casella "Modalità di sincronizzazione".

   Se non esistono ancora server NTP creare un server NTP con il pulsante "Configura server...".

5.3.3 Definire il server NTP

Definire un nuovo server NTP nel modo seguente:

1. Inserire un nome utente per il server NTP.



2. Inserire l'indirizzo IP / l'FQDN del server NTP.
3. Selezionare il tipo.

Impostazioni per NTP (protetto)

1. Fare clic sul pulsante "Aggiungi...".
2. Inserire i seguenti dati:

Parametri	Significato
ID chiave	Valore numerico tra 1 ... 65534.
Autenticazione	Selezionare la modalità di autenticazione.
Hex/ASCII	Selezionare il formato per la chiave NTP.
Chiave	Inserire la chiave NTP della seguente lunghezza: Hex: 22 ... 40 caratteri ASCII: 11 ... 20 caratteri

Importazione / esportazione di server NTP

Con i pulsanti "Importa..." o "Esporta..." è possibile esportare l'elenco delle chiavi del server NTP attualmente visualizzato e importare il file in un server NTP o viceversa.

5.4 SNMP

5.4.1 Informazioni generali

Cos'è SNMP?

L'unità Security supporta la trasmissione di informazioni di gestione tramite il Simple Network Management Protocol (SNMP). Per questo motivo sull'unità Security è installato un "SNMP Agent" che accetta e risponde alle richieste SNMP. Le informazioni sulle proprietà degli apparecchi con funzionalità SNMP si trovano nei cosiddetti file MIB (Management Information Base) per i quali l'utente deve disporre dei diritti necessari (SNMPv3).

Con SNMPv1 la "Stringa Community" viene inviata insieme. La "Stringa Community" è come una password che viene inviata insieme alla richiesta SNMP. Se la stringa Community è corretta, l'unità Security risponde con l'informazione richiesta. Se la stringa è errata, l'unità Security respinge la richiesta e non risponde.

Con SNMPv3 i dati possono essere trasmessi senza codifica.

5.4.2 Attiva SNMP

Requisito richiesto

Config. HW: Nella scheda "SNMP" delle proprietà del CP è attivata la casella di controllo "Attiva SNMP". Se questa casella non è attivata, SNMP non può essere configurato nel Security Configuration Tool. CP

Configurazione di SNMP - Procedimento:

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "SNMP"
3. Attivare la casella di controllo "Attiva SNMP". SCA. S
4. Selezionare una delle versioni di protocollo SNMP:

Nota

Trasmissione dei dadi codificata in SNMPv3

Per aumentare la sicurezza è necessario utilizzare SNMPv3 in quanto i dati vengono trasmessi codificati.

- SNMPv1

  Per controllare i diritti di accesso nell'SNMO Agent l'unità Security utilizza i seguenti valori standard per le stringhe Community:

  Per l'accesso in lettura: public

  Per l'accesso in lettura e in scrittura: private

  Per attivare l'accesso in scrittura tramite SNMP attivare la casella opzione "Consenti accesso in scrittura'".

- SNMPv3

  Selezionare un metodo di autenticazione o un metodo di autenticazione e codifica.

  Algoritmo di autenticazione: nessuno, MD5, SHA-1

  Algoritmo di codifica: nessuno, AES-128, DES

Nota

Evitare l'utilizzo di DES

DES è un algoritmo di codifica non protetto. Di conseguenza deve essere utilizzato per motivi di compatibilità inversa.

Nota

In caso di impiego di SNMPv3 non è possibile un'autenticazione RADIUS.

5. Configurare nell'area "Impostazioni estese" i dati specifici per l'unità relativi all'autore, la posizione e l'indirizzo e-mail che sovrascrivono le indicazioni delle proprietà del progetto. Se si attiva la casella di controllo "Mantieni valori scritti con il set SNMP", i valori scritti sull'unità Security da uno strumento SNMP tramite un comando SNMP-SET non vengono sovrascritti dal caricamento di una configurazione da SCT all'unità Security. SCA. S
6. Se deve essere utilizzato SNMPv3, assegnare ad un utente un ruolo per il quale sono attivati i diritti SNMP corrispondenti, in modo che esso possa raggiungere l'unità Security tramite SNMP.

   Per maggiori informazioni sulla configurazione di utenti, diritti e ruoli, vedere il seguente capitolo:

   – Gestione degli utenti (Pagina 64)

5.5 Proxy ARP

S≥V3.0

Informazioni generali

Proxy ARP consente ai router di rispondere alle richieste ARP per host. Gli host si trovano quindi nelle reti separate da router, ma utilizzano tuttavia la stessa area di indirizzi IP.

Se il PC1 invia una richiesta ARP al PC2, esso riceve una risposta ARP dall'unità Security intermedia e non dal PC2 e l'indirizzo hardware dell'interfaccia (indirizzo MAC della porta sull'unità Security), sulla quale è stata ricevuta la richiesta. Il PC1 richiedente invia quindi i suoi dati all'unità Security che li inoltra successivamente al PC2.

A questa funzione si accede nel modo seguente

Questa funziona è disponibile solo per l'interfaccia interna di un'unità Security, che è un nodo di un gruppo VPN e che si trova in modalità Bridge. Inoltre il progetto deve trovarsi in modalità estesa.

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "ARP Proxy"
3. Se l'unità deve rispondere ad una richiesta ARP dalla propria LAN in sostituzione ad un partner specifico del collegamento, inserire l'indirizzo IP corrispondente.

Comunicazione protetta nella VPN tramite tunnel IPsec

6

In questo capitolo è descritto come collegare sottoreti IP protette dall'unità Security o SCALANCE M ad una VPN (Virtual Private Network).

Come già descritto nel capitolo relativo alle proprietà dell'unità, anche in questo caso è possibile consentire impostazioni standard per utilizzare una comunicazione sicura nelle reti interne.

Altre informazioni

Le informazioni dettagliate sulle finestre di dialogo e i parametri impostabili si trovano anche nella guida in linea.

Alla guida è possibile accedere con il tasto F1 o con il pulsante "Help" nella relativa finestra di dialogo.

Vedere anche

Funzioni online - Diagnostica e logging (Pagina 249)

6.1 VPN con unità Security e SCALANCE M

Collegamento protetto tramite rete non protetta

Per le unità Security e SCALANCE M, che proteggono la rete interna, i tunnel IPsec mettono a disposizione un collegamento di dati protetto attraverso la rete esterna non sicura.

Grazie allo scambio di dati tramite IPsec, per la comunicazione vengono realizzati i seguenti aspetti di sicurezza:

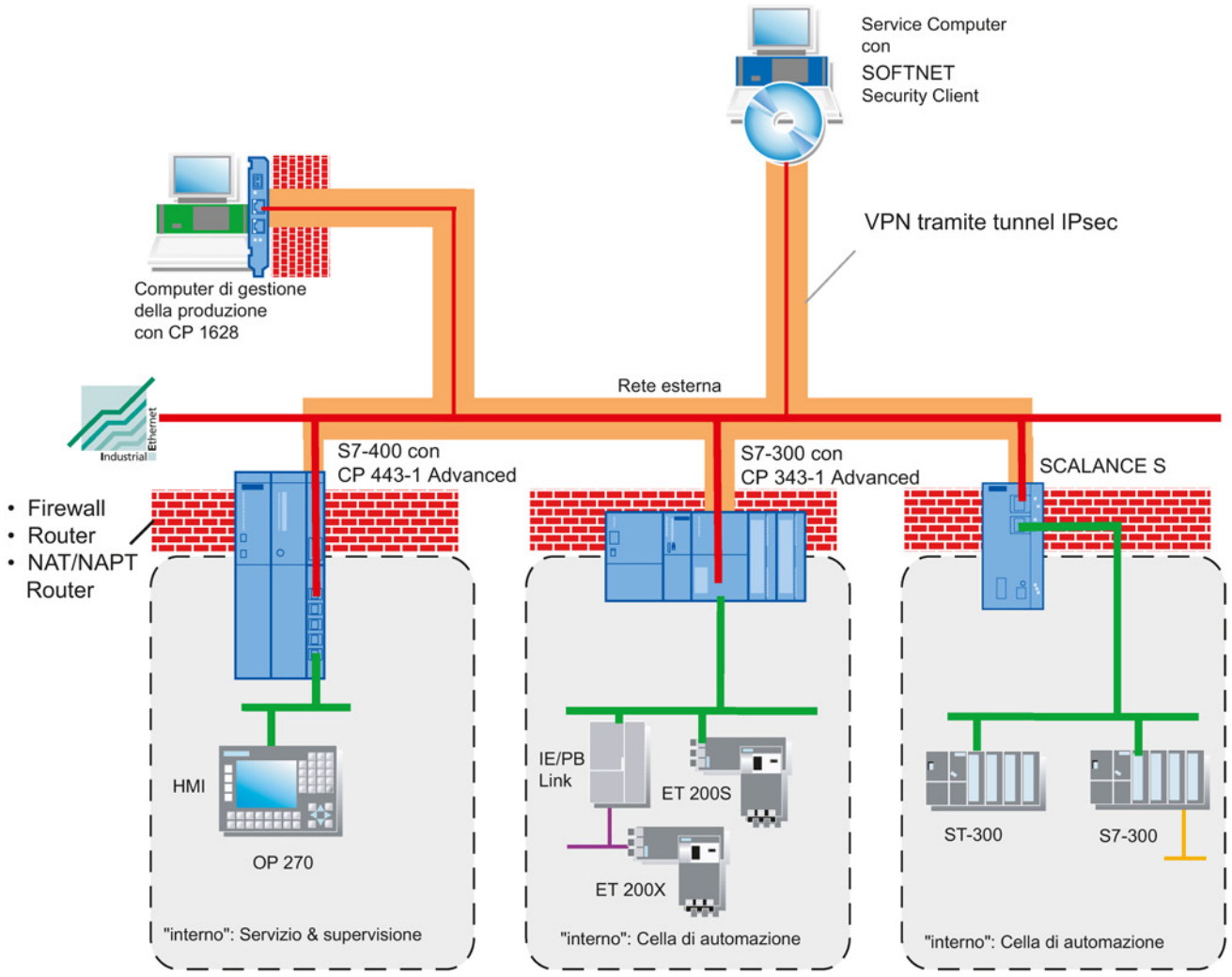
- Riservatezza

  Garantisce che i dati possano essere trasmessi senza codifica.
- Integrità

  Garantisce che i dati non siano stati modificati.
- Autenticità

  Garantisce che i punti terminali VPN siano anche fidati.

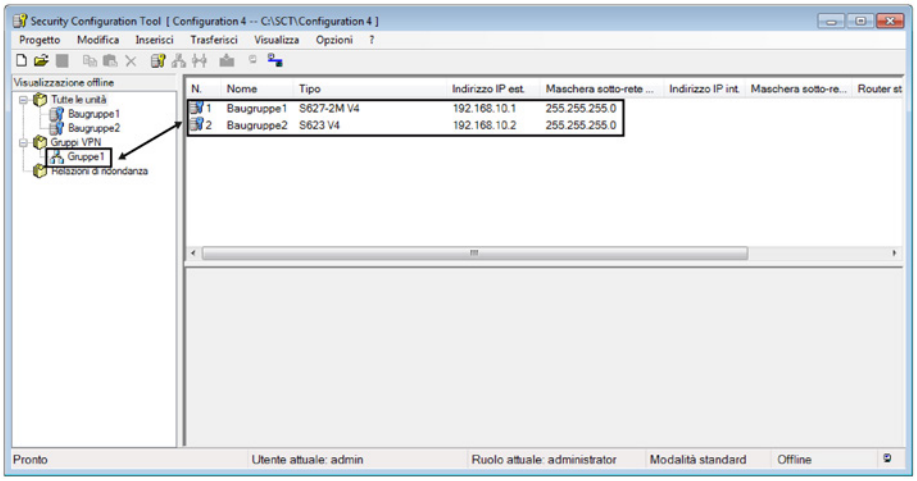
Per la realizzazione dei tunnel l'unità utilizza il protocollo IPsec (modalità tunnel di IPsec).



Collegamenti tramite tunnel in atto tra unità dello stesso gruppo VPN

Nelle unità le proprietà di una VPN vengono riunite in un gruppo VPN per tutti i tunnel IPsec.

I tunnel IPsec vengono realizzati automaticamente tra tutte le unità e i SOFTNET Security Client appartenenti allo stesso gruppo VPN. In questo caso un'unità in un progetto può appartenere parallelamente a diversi gruppi VPN.


Security Configuration Tool [Configuration 4 -- C:\SCT\Configuration 4]
Progetto Modifica Inserisci Trasferisci Visualizza Opzioni ?
Visualizzazione offline
Tutte le unità
Baugruppe1
Baugruppe2
Gruppi VPN
Gruppe1
Relazioni di ridondanza
N. Nome Tipo Indirizzo IP est. Maschera sotto-rete ... Indirizzo IP int. Maschera sotto-re... Router st
1 Baugruppe1 S627-2M V4 192.168.10.1 255.255.255.0
2 Baugruppe2 S623 V4 192.168.10.2 255.255.255.0
Pronto
Utente attuale: admin
Ruolo attuale: administrator
Modalità standard
Offline

Nota

Se viene modificato il nome di un'unità, è necessario riconfigurare tutte le unità dei gruppi VPN dei quali fa parte l'unità modificata (voce di menu "Trasferisci" > "A tutte le unità...").

Se viene modificato il nome di un gruppo VPN, è necessario riconfigurare tutte le unità di questo gruppo VPN (voce di menu "Trasferisci" > "A tutte le unità...").

Nota

I telegrammi layer 2 vengono trasmessi anche via tunnel se tra due unità si trova un router. A tal proposito gli indirizzi MAC del partner di comunicazione devono tuttavia essere configurati in modo statico nel Security Configuration Tool ed eventualmente le voci APR statiche devono essere inserite negli apparecchi di comunicazione.

In generale vale quanto segue: i telegrammi non-IP vengono trasmessi attraverso il tunnel solo se gli apparecchi, che inviano e ricevono telegrammi, potevano comunicare già prima senza l'impiego di unità.

6.2 Metodo di autenticazione

Metodo di autenticazione

Il metodo di autenticazione viene definito all'interno di un gruppo VPN e determina il tipo di autenticazione utilizzata.

Vengono supportati metodi di autenticazione basati su codifica o basati su certificato:

- Preshared Keys

  L'autenticazione avviene tramite una sequenza di caratteri precedentemente elaborata che viene ripartita su tutte le unità che si trovano nel gruppo VPN.

  Inserire quindi nella finestra di dialogo "Proprietà del gruppo VPN" nella casella "Chiave" una password o generare una nuova password con il pulsante "Nuovo...".

- Certificato

  L'autenticazione basata sul certificato "Certificato" è l'impostazione standard attivata anche in modalità standard. Il comportamento è il seguente:

  – Durante la creazione di un gruppo VPN, per il gruppo VPN viene generato automaticamente un certificato CA.

  – Ogni unità, che si trova nel gruppo VPN, riceve un certificato di gruppo VPN firmato con la chiave dell'autorità di certificazione del gruppo VPN.

  Tutti i certificati sono basati sullo standard ITU X.509v3 (ITU, International Telecommunications Union).

  I certificati vengono generati da una posizione di certificazione contenuta in un Security Configuration Tool.

Nota

Limitazioni in caso di funzionamento VLAN

Nei telegrammi IP attraverso il tunnel VPN dell'unità non viene trasmesso nessun tagging VLAN. I tag VLAN contenuti nei telegrammi IP vengono persi attraversando le unità in quanto per la trasmissione dei telegrammi IP viene utilizzato IPsec.

Come standard con IPsec non possono essere trasmessi telegrammi IP-Broadcast o IP-Multicast attraverso un tunnel VPN layer 3. Attraverso un tunnel VPN layer 2 VPN dell'unità Security i telegrammi IP o i telegrammi IP-Multicast vengono "compressi" e trasmessi esattamente come pacchetti MAC compresa l'intestazione Ethernet in UDP. Di conseguenza in questi pacchetti viene mantenuto il VLAN Tagging.

6.3 Gruppi VPN

6.3.1 Regole per la formazione di gruppi VPN

Osservare le seguenti regole.

- Per SCALANCE S612 / S613 / S623 / S627-2M / SCALANCE M / dispositivo VPN

  La prima unità assegnata in un gruppo VPN determina le unità aggiuntive che possono essere inserite.

  Se la prima unità SCALANCE S aggiunta è in modalità Routing o se la prima unità è un'unità SCALANCE M o un dispositivo VPN, possono inoltre essere aggiunti solo unità SCALANCE S con Routing attivato o unità SCALANCE M o dispositivi VPN, poiché le unità SCALANCE M e i dispositivi VPN possono essere utilizzati solo in modalità Routing.
  Se la prima unità SCALANCE S aggiunta è in modalità Bridge, è possibile aggiungere inoltre solo unità SCALANCE S in modalità Bridge.
  Un CP, un SSC e un NCP client VPN (Android) può essere aggiunto ad un gruppo VPN con uno SCALANCE S in modalità Bridge o Routing.

- Per CP / SSC / NCP client VPN (Android)

  Se un CP / SSC / NCP client VPN (Android) è il primo in un gruppo VPN, le unità possono essere aggiunte in una modalità qualsiasi, tranne un'unità SCALANCE S o SCALANCE M. A partire da questo momento valgono le regole per unità SCALANCE S e SCALANCE M, vedere sopra.

- Non è possibile aggiungere un'unità SCALANCE M ad un gruppo VPN che contiene un'unità SCALANCE S in modalità Bridge.

Rilevare dalla seguente tabella quali unità possono essere inclusi in un gruppo VPN:

Tabella 6- 1 Regole per la formazione di gruppi VPN

Unità	Può essere acquisita nel gruppo VPN con le seguenti unità contenute:		
	SCALANCE S in modalità Bridge	SCALANCE S in modalità Routing / SCALANCE M / dispositivo VPN / NCP client VPN (Android)	CP / SSC
SCALANCE S in modalità Bridge	x	-	x
SCALANCE S in modalità Routing	-	x	x
CP x43-1 Adv.	x	x	x
CP 1628	x	x	x
SOFTNET Security Client 2005	x	-	-
SOFTNET Security Client 2008	x	x	x
SOFTNET Security Client V3.0	x	x	x

Unità	Può essere acquisita nel gruppo VPN con le seguenti unità contenute:		
	SCALANCE S in modalità Bridge	SCALANCE S in modalità Routing / SCALANCE M / dispositivo VPN / NCP client VPN (Android)	CP / SSC
SOFTNET Security Client V4.0	x	x	x
SCALANCE M / apparecchio VPN	-	x	x
NCP VPN Client (Android)	-	x	x

6.3.2 Rapporti di comunicazione via tunnel supportati

Significato

Le seguenti tabelle indicano quali interfacce tunnel possono realizzare tra loro un tunnel. Si distingue quindi se l'unità SCALANCE S si trova in modalità Routing o in modalità Bridge.

Indipendentemente dall'interfaccia tramite la quale viene realizzato il tunnel VPN, come standard i nodi delle sottoreti interne delle unità Security possono comunicare sempre tra loro. Se la comunicazione tramite il tunnel VPN deve essere eseguita anche in altre sottoreti, esse possono essere abilitate dalla scheda "VPN" nelle proprietà estese dell'unità per la comunicazione via tunnel, vedere il seguente capitolo:

- Configurazione di ulteriori nodi e sottoreti per il tunnel VPN (Pagina 217)

Le sottoreti che devono essere abilitate per la comunicazione via tunnel sono:

- Sottorete sull'interfaccia esterna (se l'interfaccia esterna non è il punto terminale VPN)
- Sottorete sull'interfaccia DMZ (se l'interfaccia DMZ non è il punto terminale VPN)
- Ulteriori sottoreti raggiungibili tramite router su diverse interfacce (se esse non sono punti terminali VPN)

Tabella 6- 2 Comunicazione via tunnel tra CP, unità SCALANCE M, SOFTNET Security Client e unità SCALANCE S in modalità Routing

	Interfaccia Responder				
Interfaccia Initiator	Esterno (SCALANCE M875)	Esterno (SCALANCE M-800)	GBit, IE (CP)	Esterno (SCALANCE S)	DMZ (SCALANCE S623 / S627-2M)
PC/PG (SSC)	x	x	x	x	x
Esterno (SCALANCE M875)	-	x	x	x	x

	Interfaccia Responder				
Interfaccia Initiator	**Esterno (SCALANCE M875)**	**Esterno (SCALANCE M-800)**	**GBit, IE (CP)**	**Esterno (SCALANCE S)**	**DMZ (SCALANCE S623 / S627-2M)**
Esterno (SCALANCE M-800)	-	**x**	**x**	**x**	**x**
GBit, IE (CP)	-	-	**x**	**x**	**x**
Esterno (SCALANCE S)	-	-	**x**	**x**	**x**
DMZ (SCALANCE S623 / S627-2M)	-	-	**x**	**x**	**x**

x è supportato

- non è supportato

Tabella 6- 3 Comunicazione via tunnel tra CP, SOFTNET Security Client e unità SCALANCE S in modalità Bridge

	Interfaccia Responder		
Interfaccia Initiator	**GBit, IE (CP)**	**Esterno (SCALANCE S)**	**DMZ (SCALANCE S623 / S627-2M)**
PC/PG (SSC)	**x**	**x**	-
GBit, IE (CP)	**x**	**x**	-
Esterno (SCALANCE S)	**x**	**x**	-
DMZ (SCALANCE S623 / S627-2M)	-	-	-

x è supportato

- non è supportato

6.3.3 Creazione di gruppi VPN e assegnazione e assegnazione di unità

Requisito richiesto

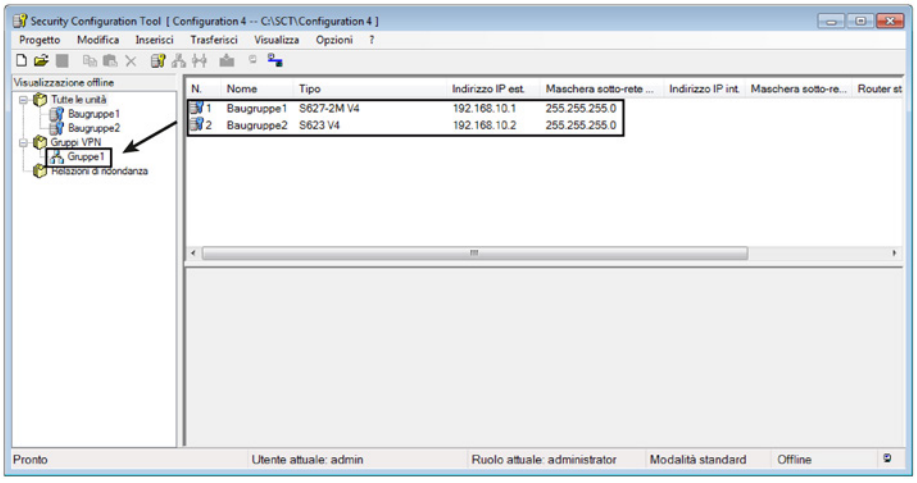
Nota

Data attuale e ora attuale sulle unità

In caso di utilizzo di comunicazione protetta (ad es. HTTPS, VPN...) fare attenzione che le unità interessate dispongano dell'ora e della data attuale. I certificati utilizzati vengono altrimenti valutati non validi e la comunicazione protetta non funziona.

A questa funzione si accede nel modo seguente

1. Creare un gruppo VPN dalla voce di menu "Inserisci" > "Gruppo".
2. Assegnare al gruppo VPN le unità, i SOFTNET Security Client, i dispositivi VPN e i client VPN NCP (Android) che devono appartenere ad un gruppo VPN. Trascinare quindi con il mouse l'unità nell'area del contenuto sul gruppo VPN desiderato nell'area di navigazione (Drag and Drop).


Security Configuration Tool [Configuration 4 -- C:\SCT\Configuration 4]
Progetto Modifica Inserisci Trasferisci Visualizza Opzioni ?
Visualizzazione offline
Tutte le unità
Baugruppe1
Baugruppe2
Gruppi VPN
Gruppe1
Relazioni di ridondanza
N. Nome Tipo Indirizzo IP est. Maschera sotto-rete ... Indirizzo IP int. Maschera sotto-re... Router st
1 Baugruppe1 S627-2M V4 192.168.10.1 255.255.255.0
2 Baugruppe2 S623 V4 192.168.10.2 255.255.255.0
Pronto
Utente attuale: admin
Ruolo attuale: administrator
Modalità standard
Offline

Progettazione delle proprietà

Come per la configurazione delle unità, anche per la configurazione dei gruppi VPN le due visualizzazioni di comando selezionabili hanno effetto nel Security Configuration Tool:

- **Modalità standard**

  In modalità standard lasciare le preimpostazioni eseguite dal sistema. Anche come non esperti è possibile configurare tunnel IPsec e utilizzare una comunicazione di dati sicura.

- **Modalità estesa**

  La modalità estesa offre le possibilità di impostazione per la configurazione specifica della comunicazione via tunnel.

Visualizzazione di tutti i gruppi VPN progettati con relative proprietà

- Selezionare l'oggetto "Gruppi VPN" nell'area di navigazione.

Le seguenti proprietà dei gruppi vengono visualizzate per colonne:

Proprietà/colonna	Significato	Commento/selezione
Name	Nome del gruppo	Selezionabile liberamente
Authentification	Tipo di autenticazione	• Preshared Key • Certificato
Appartenenza al gruppo fino a	Durata dei certificati	Vedere sezione "Impostazione della durata dei certificati"
Comment	Commento	Selezionabile liberamente

Creazione della durata dei certificati

Aprire la finestra di dialogo, nella quale è possibile inserire la data di scadenza del certificato, nel modo seguente:

1. Selezionare nell'area di navigazione il relativo gruppo VPN per il quale si vuole configurare un certificato.
2. Fare clic con il tasto destro del mouse sull'unità nell'area del contenuto e selezionare il comando "Nuovo certificato..." nel menu di scelta rapida.

Nota

Scadenza di un certificato

Allo scadere del certificato la comunicazione attraverso il VPN prosegue fino a quando il tunnel viene interrotto o la durata SA è scaduta. Ulteriori informazioni sui certificati si trovano nel seguente capitolo:

- Gestione dei certificati (Pagina 80)

6.4 Configurazione del tunnel nella modalità Standard

Apertura della finestra di dialogo per la visualizzazione dei valori standard

1. Contrassegnare il gruppo VPN.
2. Selezionare la voce di menu "Edit" > "Properties...".

La visualizzazione delle proprietà del gruppo VPN è identica alla visualizzazione in modalità estesa, i valori non possono tuttavia essere modificati in modalità standard.

6.5 Configurazione del tunnel in modalità estesa

La modalità estesa offre le possibilità di impostazioni per la configurazione specifica della comunicazione via tunnel.

Commutazione nella modalità estesa

Attivare il progetto per tutte le funzioni descritte in questo capitolo in modalità estesa.

Nota

Non è possibile una ricommutazione alla modalità standard

Non appena è stata modificata la configurazione per il progetto attuale, non è più possibile annullare una commutazione nella modalità estesa precedentemente eseguita.

Rimedio SCT Standalone: chiudere il progetto senza salvarlo e aprirlo di nuovo.

6.5.1 Progettazione delle proprietà del gruppo VPN

Proprietà dei gruppi VPN

Nota

Nozioni IPsec necessarie

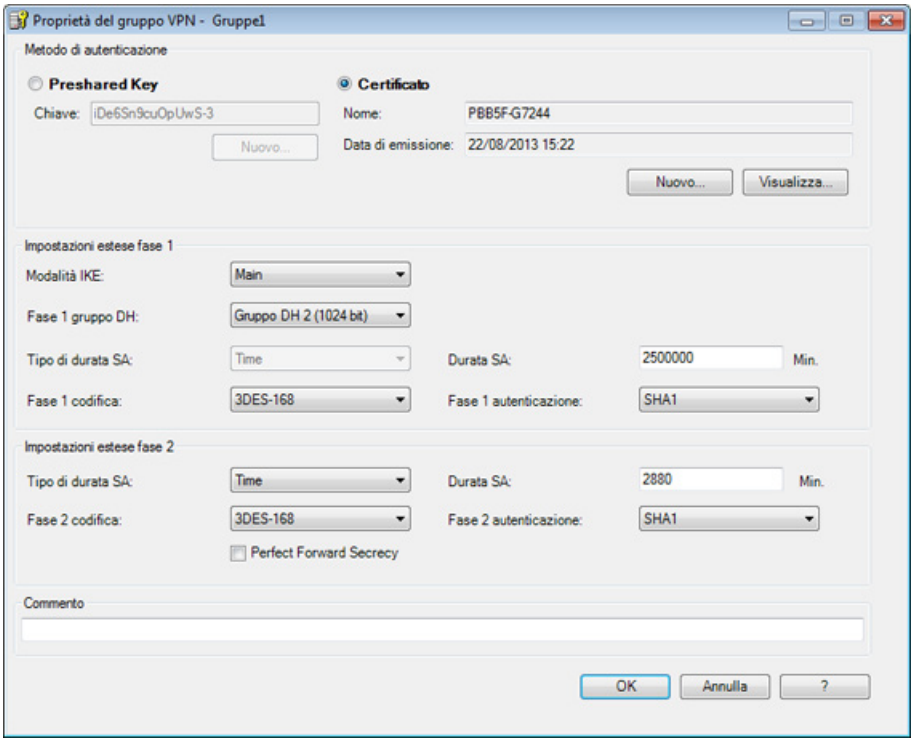
Per poter impostare questi parametri è necessario conoscere IPsec. Se non si eseguono o modificano impostazioni, valgono le impostazioni standard della modalità standard.

In modalità estesa possono essere progettate le seguenti proprietà del gruppo VPN:

- Metodo di autenticazione
- Impostazioni IKE (campo finestra di dialogo: Advanced Settings Phase 1)
- Impostazioni IPsec (campo finestra di dialogo: Advanced Settings Phase 2)

A questa funzione si accede nel modo seguente

1. Selezionare il gruppo VPN da modificare nella modalità estesa.
2. Selezionare la voce di menu "Modifica" > "Proprietà...".



3. Selezionare se per l'autenticazione deve essere utilizzata una Preshared Key o un certificato. Ulteriori informazioni su questo argomento si trovano nel seguente capitolo:
   – Metodo di autenticazione (Pagina 194).

Parametri per impostazioni avanzate fase 1

Phase 1: Negoziazione IKE della Security Association (SA) per fase 2:

Impostare qui i parametri per la negoziazione dei parametri di sicurezza che vengono utilizzati nella fase 2:

Parametri	Descrizione
Modalità IKE	• Modalità Main • Modalità Aggressive La differenza tra Main Mode e Aggressive Mode è la "identity protection" che viene utilizzata nel Main Mode. L'identità viene trasmessa codificata nel Main Mode, mentre nell'Aggressive Mode non viene trasmessa.
Fase 1 gruppo DH	Gruppi selezionabili per lo scambio di chiave Diffie-Hellman: • Group 1 • Group 2 • Group 5 • Group 14
Tipo di durata SA	Phase 1 Security Association (SA): • Time: Limitazione del tempo in minuti La durata utile per il materiale attuale codificato viene limitata a tempo. Allo scadere del tempo il materiale codificato viene di nuovo concordato.
Durata SA	Valore numerico: Campo di valori per time: 1440 ... 2500000 minuti (standard: 2500000)
Fase 1 codifica	Algoritmo di codifica: • DES*: Data Encryption Standard (lunghezza codice 56 bit, modalità CBC) • 3DES-168: DES triplo (lunghezza codice 168 bit, modalità CBC) • AES-128, 192, 256: Advanced Encryption Standard (lunghezza codice 128, 192 bit o 256 bit, modalità CBC)
Fase 1 autenticazione	Algoritmo di autenticazione • MD5: Message Digest Algorithm 5 • SHA1: Secure Hash Algorithm 1

* DES è un algoritmo di codifica non sicuro. Esse deve essere utilizzato solo per motivi di compatibilità inversa.

Parametri per impostazioni avanzate fase 2

Fase 2: Negoziazione IKE della Security Association (SA) per lo scambio di dati IPsec:

Impostare qui i parametri per la negoziazione dei parametri di sicurezza che vengono utilizzato per lo scambio di dato IPsec con ESP (Encapsulating Security Payload) e AH (Authentication Header). La comunicazione nella 2 avviene già codificata.

Parametri	Descrizione
Tipo di durata SA	Phase 2 Security Association (SA): • Time: La limitazione di tempo in minuti La durata utile per il materiale attuale codificato viene limitata a tempo. Allo scadere del tempo il materiale codificato viene di nuovo concordato. • Limite: Limitazione del volume di dati in Mbyte
Durata SA	Valore numerico: • Campo di valori per time: 60 ... 16666666 minuti (standard: 2880) • Campo di valori per Limit: 2000 ... 500000 Mbyte (standard: 4000)
Fase 2 codifica	Algoritmo di codifica: • DES*: Data Encryption Standard (lunghezza codice 56 bit, modalità CBC) • 3DES-168: DES triplo (lunghezza codice 168 bit, modalità CBC) • AES-128: Advanced Encryption Standard (lunghezza codice 128 bit, modalità CBC)
Fase 2 autenticazione	Algoritmo di autenticazione • MD5: Message Digest Algorithm 5 • SHA1: Secure Hash Algorithm 1
Perfect Forward Secrecy	Se si attiva questa casella di controllo, per il ricalcolo della chiave vengono scambiati nuovi Diffie Hellmann Public Key Values. Se si disattiva la casella di controllo, per il ricalcolo della chiave vengono utilizzai i valori già scambiati nella fase 1.

* DES è un algoritmo di codifica non sicuro. Esse deve essere utilizzato solo per motivi di compatibilità inversa.

6.5.2 Acquisizione dell'unità nel gruppo VPN configurato

Le proprietà del gruppo progettate vengono acquisite per le unità inserite in un gruppo VPN esistente.

Inserimento di nodi attivi in un gruppo VPN

Se un nodo attivo viene aggiunto in un gruppo VPN esistente, esso può raggiungere i nodi del gruppo senza dover ricaricare il progetto su tutti i nodi del gruppo VPN.

Nota

Se si rimuove un nodo attivo da un gruppo VPN esistente, esso può sempre realizzare un collegamento con i nodi del gruppo, anche se il progetto è stato di nuovo caricato su tutti i nodi del gruppo VPN.

Se il nodo attivo remoto non deve più poter realizzare un collegamento, rinnovare il certificato CA del gruppo VPN e caricare di nuovo il progetto sui nodi del gruppo VPN.

Il certificato CA del gruppo VPN può essere rinnovato nelle proprietà del gruppo VPN o nel manager certificati, scheda "Autorità di certificazione".

Procedimento

Durante l'inserimento è necessario distinguere quanto segue:

- **Caso a:** Se non sono state modificate le proprietà dei gruppi e l'unità da aggiungere ha realizzato il collegamento in modo attivo con le unità già configurate:

1. Aggiungere la nuova unità al gruppo VPN.
2. Caricare la configurazione sulla nuova unità.

- **Caso b:**Se non sono state modificate le proprietà dei gruppi o l'unità da aggiungere ha realizzato il collegamento in modo non attivo con le unità Security già configurate:

1. Aggiungere la nuova unità al gruppo VPN.
2. Caricare la configurazione in tutte le unità che appartengono al gruppo VPN.

Vantaggio nel caso a

Le unità già esistenti e messe in servizio non devono essere progettate e caricate di nuovo. La comunicazione in atto non viene influenzata o interrotta.

Impostazioni per nodi con indirizzo IP sconosciuto

I nodi nei quali l'indirizzo IP è sconosciuto al momento della progettazione (Unknown Peers), possono essere inseriti in un gruppo VPN esistente. Poiché per la maggior parte dei casi i nodi si trovano nell'impiego mobile e gli indirizzi IP vengono rilevati dinamicamente (ad es. un SOFTNET Security Client o uno SCALANCE M), il tunnel VPN può essere realizzato solo se le impostazioni dei parametri per la fase 1 vengono eseguite in base ad una delle seguenti tabelle. Se si utilizzano altre impostazioni non è possibile realizzare un tunnel VPN con il terminale di dati.

Tabella 6- 4 Parametri di codifica 1

Parametri	Impostazione
Fase 1 codifica	AES-256
Fase 1 gruppo DH	Group2
Fase 1 autenticazione	SHA1
Metodo di autenticazione	Certificato
Durata SA	1440 … 2500000 minuti

Tabella 6- 5 Parametri di codifica 2

Parametri	Impostazione
Fase 1 codifica	3DES-168
Fase 1 gruppo DH	Group2
Fase 1 autenticazione	SHA1
Metodo di autenticazione	Certificato
Durata SA	1440 … 2500000 minuti

Tabella 6- 6 Parametri di codifica 3

Parametri	Impostazione
Fase 1 codifica	DES
Fase 1 gruppo DH	Group2
Fase 1 autenticazione	MD5
Metodo di autenticazione	Certificato
Durata SA	1440 … 2500000 minuti

Tabella 6- 7 Parametri di codifica 4

Parametri	Impostazione
Fase 1 codifica	3DES-168
Fase 1 gruppo DH	Group2
Fase 1 autenticazione	SHA1

Parametri	Impostazione
Metodo di autenticazione	Preshared Key
Durata SA	1440 … 2500000 minuti

Limitazioni supplementari per il SOFTNET Security Client

Per il SOFTNET Security Client valgono inoltre le seguenti limitazioni:

Parametri	Impostazione / particolarità
Fase 1 codifica	AES-256 possibile solo con Windows 7
Fase 1 durata SA	1440 ... 2879 minuti
Tipo di durata SA	Deve essere selezionato identico per entrambe le fasi
Fase 2 codifica	nessun AES-128 possibile
Fase 2 durata SA	60 ... 2879 minuti
Fase 2 autenticazione	Nessun MD5 possibile

6.5.3 Progettazione delle proprietà VPN specifiche per l'unità

Significato

Per lo scambio dei dati tramite IPsec-Tunnel nella VPN è possibile configurare le seguenti proprietà specifiche per l'unità:

- Dead Peer Detection SCALANCE M
- Autorizzazione per l'inizializzazione della realizzazione del collegamento M875
- Indirizzo IP WAN / FQDN per la comunicazione tramite Internet Gateway M875
- Configurazione di nodi VPN SCALANCE M

Requisiti richiesti

- Nella scheda "VPN" le impostazioni possono essere eseguite solo se l'unità configurata si trova in un gruppo VPN.
- Il campo della finestra di dialogo "Nodi VPN" nella scheda "VPN" viene visualizzato solo se il progetto si trova in modalità estesa. SCALANCE M

A questa funzione si accede nel modo seguente

1. Selezionare l'unità da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "VPN"

   Le impostazioni qui eseguite vengono acquisite come standard come impostazioni estese all'unità per le impostazioni specifiche per il collegamento. Le impostazioni specifiche per

il collegamento possono sovrascrivere impostazioni estese all'unità e sono configurabili nella finestra dei dettagli. Ulteriori informazioni relative alla progettazione di impostazioni specifiche per il collegamento si trovano nel seguente capitolo:
Progettazione delle proprietà VPN specifiche per il collegamento (Pagina 208)

Dead-Peer-Detection (DPD) SCALANCE M

Come standard DPD è disattivato. Per consentire che DPD funzioni in modo affidabile, su entrambe le unità Security essa deve essere attivata.

Con la DPD attivata le unità Security scambiano ulteriori messaggi ad intervalli impostabili se attualmente non è in atto uno scambio di dati tramite tunnel VPN. In questo modo è possibile riconoscere se il collegamento IPsec è ancora valido o se deve eventualmente essere realizzato di nuovo. Se non è più in atto nessun collegamento, le "Security Associations" (SA) viene terminate prima dalla fase 2. Con il DPD disattivato la SA viene chiusa solo dopo che è trascorsa la durata SA. Per l'impostazione della durata SA vedere il seguente capitolo: Progettazione delle proprietà del gruppo VPN (Pagina 200).

Autorizzazione per l'inizializzazione della realizzazione del collegamento

L'autorizzazione per l'inizializzazione di realizzazione del collegamento VPN può essere limitata a determinate unità nella VPN.

Per l'impostazione del parametro descritto è indicativa l'assegnazione dell'indirizzo per il Gateway dell'unità da progettare. Con un indirizzo IP statico, l'unità può essere trovata dal punto opposto. Con un indirizzo IP dinamico, e quindi sempre diverso, il punto opposto non può realizzare un collegamento.

Modalità	Significato
Avvio del collegamento senza punto opposto (Initiator/Responder) (standard)	Con questa opzione l'unità è "attiva", cioè tenta di realizzare un collegamento con un punto opposto. È inoltre possibile anche l'accettazione di richieste per la realizzazione del collegamento VPN. Questa opzione si raccomanda se all'unità da progettare di ISP viene assegnato un indirizzo IP dinamico. L'indirizzamento del punto opposto viene eseguito tramite il relativo indirizzo IP WAN progettato, il relativo indirizzo IP unità esterno o l'FQDN progettato.
Attesa del punto opposto (Responder)	Con questa opzione l'unità è "passiva", cioè si attende fino all'inizializzazione della realizzazione del collegamento dal punto opposto. Questa opzione si raccomanda se all'unità da progettare da ISP viene assegnato un indirizzo IP fisso.

Nota

Non impostare tutte le unità di un gruppo VPN su "Attesa del punto opposto", in quanto altrimenti non viene realizzato nessun collegamento.

Indirizzo IP WAN / FQDN - Indirizzi IP delle unità e Gateway in una VPN tramite Internet

Nel funzionamento di una VPN con IPsec Tunnel tramite Internet sono normalmente necessari indirizzi IP supplementari per gli Internet Gateway, ad es. il router DSL. Le singole unità Security o unità SCALANCE M devono conoscere gli indirizzi IP pubblici delle unità partner che devono essere raggiunte tramite Internet nella VPN.

Nota

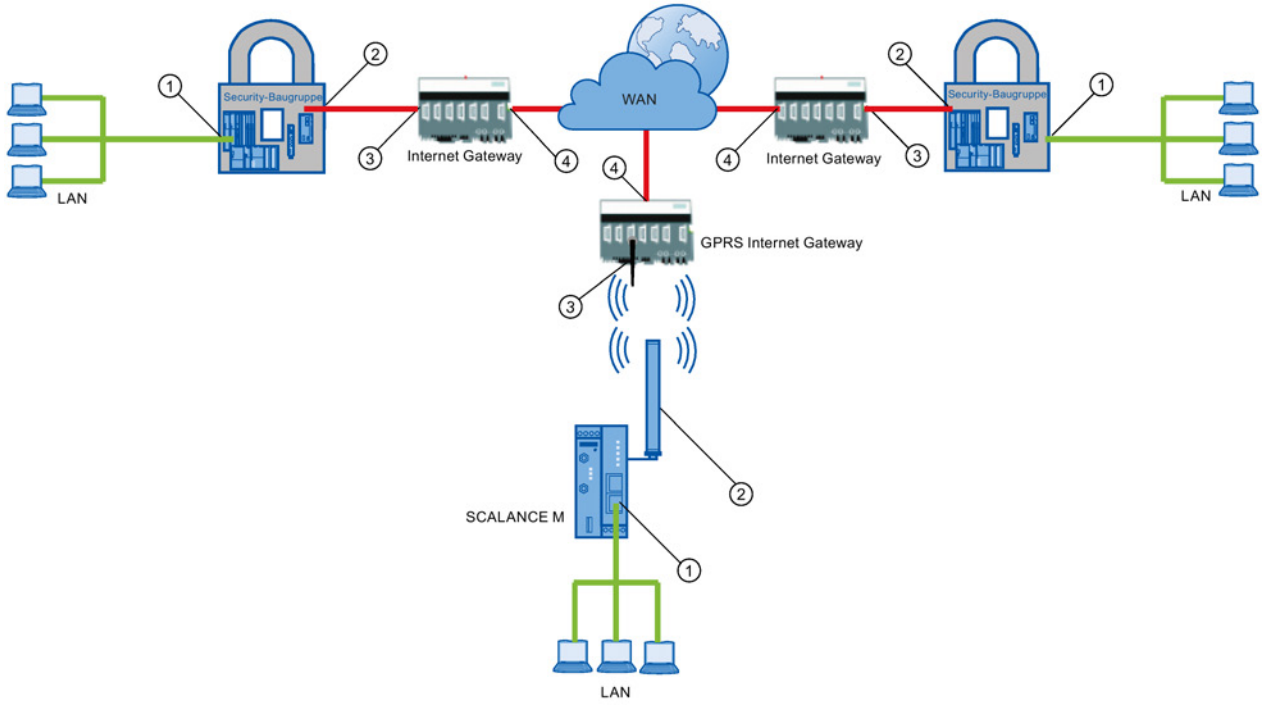
Se si utilizza un router DSL come Internet Gateway, su questo router devono essere abilitate almeno le seguenti porte in base alle indicazioni nella relativa documentazione e inoltrati i pacchetti di dati all'unità:

- Porta 500 (ISAKMP)
- Porta 4500 (NAT-T)

Per questo esiste la possibilità di definire un "Indirizzo IP WAN" nella configurazione delle unità Security o SCALANCE M. Durante il caricamento della configurazione dell'unità vengono trasmessi ai nodi del gruppo gli indirizzi IP WAN delle unità partner. In alternativa ad un indirizzo IP WAN può essere inserito anche un FQDN. Se sull'unità Security è stato configurato simultaneamente DNS dinamico, questo FQDN deve corrispondere all'FQDN inserito nella scheda "DNS", registrato da un provider per il DNS dinamico.

Nelle proprietà VPN specifiche per il collegamento è possibile definire se deve essere utilizzato l'indirizzo IP esterno, l'indirizzo IP dell'interfaccia DMZ (solo SCALANCE S623 / S627-2M) o l'indirizzo IP WAN / l'FQDN. Ulteriori informazioni relative alle proprietà VPN specifiche per il collegamento si trovano nel seguente capitolo:
Progettazione delle proprietà VPN specifiche per il collegamento (Pagina 208)

Se non viene inserito nessun punto di accesso, come punto terminale VPN viene utilizzato l'indirizzo IP esterno o l'indirizzo IP dell'interfaccia DMZ (solo SCALANCE S623/S627-2M). Per le unità SCALANCE M-800 progettate come responder è necessario indicare un punto di accesso.



① Indirizzo IP interno - di un'unità Security
② Indirizzo IP esterno - di un'unità
③ Indirizzo IP di un Internet Gateway (ad es. gateway GPRS)
④ Indirizzo IP (indirizzo IP WAN) di un Internet Gateway (ad es. router DSL)

Configurazione di nodi VPN SCALANCE M

Nell'area della finestra di dialogo "Nodi VPN" abilitare le sottoreti o i nodi per la comunicazione via tunnel VPN.

I nodi o le sottoreti che devono essere abilitati e come devono essere abilitati per la comunicazione via tunnel VPN sono descritti nei seguenti capitoli:

Configurazione di ulteriori nodi e sottoreti per il tunnel VPN (Pagina 217)

Configurazione di nodi di rete interni (Pagina 217)

6.5.4 Progettazione delle proprietà VPN specifiche per il collegamento

Significato

Mentre le proprietà VPN specifiche per l'unità sono state progettate in modo specifico per un'unità, le proprietà VPN specifiche per il collegamento si riferiscono ai collegamenti VPN di un'unità. Se un'unità realizza diversi collegamenti via tunnel con altre unità Security, è possibile configurare quali collegamenti vengono inizializzati o meno dall'unità.

Requisiti richiesti

- L'unità è un nodo di un gruppo VPN.

A questa funzione si accede nel modo seguente

1. Selezionare nell'area di navigazione il gruppo VPN al quale appartiene l'unità da modificare.
2. Selezionare nell'area del contenuto l'unità della quale si vogliono progettare le proprietà.

   Nella finestra dei dettagli è possibile progettare solo le proprietà VPN specifiche per il collegamento. I valori preimpostati sono rilevati dalle proprietà VPN specifiche per l'unità.

Parametri

Parametri	Significato
Initiator/Responder	Definizione dell'autorizzazione per l'inizializzazione della realizzazione del collegamento.
Unità partner	Indicazione del nome dell'unità partner
Tipo dei pacchetti trasmessi	Indicazione del Layer al quale vengono inviati i pacchetti.
Interfaccia locale	Definizione dell'interfaccia che deve essere utilizzata come punto terminale VPN su un'unità selezionata. Se per l'unità è progettato un punto accesso WAN (indirizzo IP / FQDN) esso può essere utilizzato anche in questo caso.
Interfaccia partner	Definizione dell'interfaccia che deve essere utilizzata come punto terminale VPN su un'unità partner. Se per il punto opposto VPN è progettato un punto accesso WAN (indirizzo IP / FQDN) esso può essere utilizzato anche in questo caso.

6.6 Dati di configurazione per le unità SCALANCE M

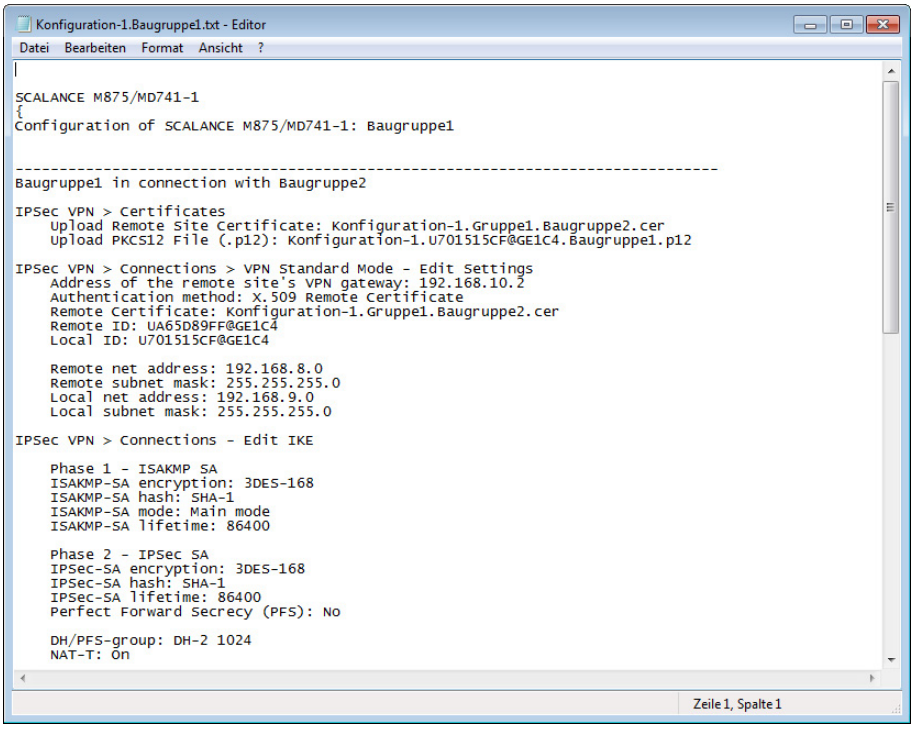
SCA. M

Significato

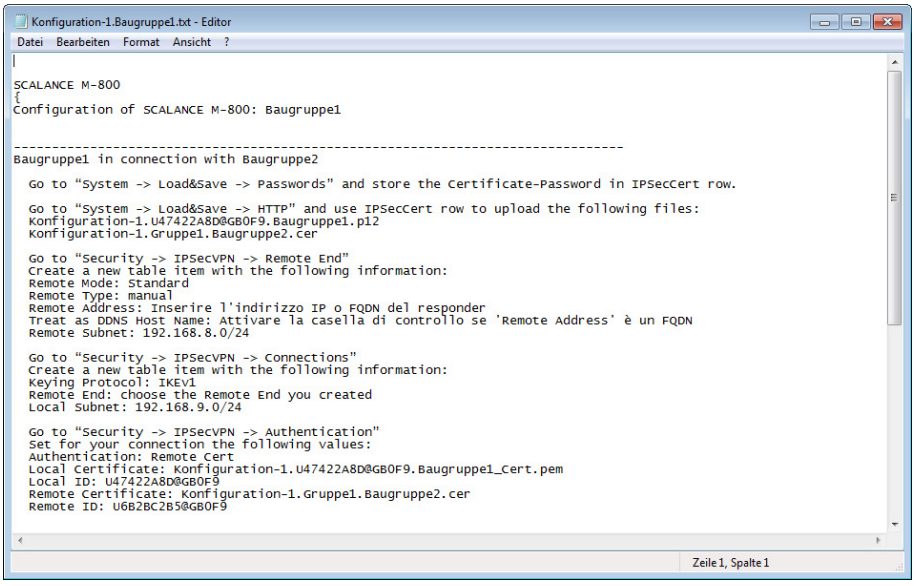
Le informazioni VPN per la parametrizzazione di unità SCALANCE M possono essere generate con il Security Configuration Tool. Con i file generati è quindi possibile configurare le unità SCALANCE M.

Vengono generati i seguenti tipi di file:

- File di esportazione con dati di configurazione
  - Tipo di file: File *.txt in formato ASCII
  - Contiene le informazioni di configurazione esportate per SCALANCE M, compresa un'informazione su ulteriori certificati generati.
  - File di esportazione per unità SCALANCE M875:


Konfiguration-1.Baugruppe1.txt - Editor
Datei Bearbeiten Format Ansicht ?
SCALANCE M875/MD741-1
{
Configuration of SCALANCE M875/MD741-1: Baugruppe1
Baugruppe1 in connection with Baugruppe2
IPSec VPN > Certificates
Upload Remote Site Certificate: Konfiguration-1.Gruppe1.Baugruppe2.cer
Upload PKCS12 File (.p12): Konfiguration-1.U701515CF@GE1C4.Baugruppe1.p12
IPSec VPN > Connections > VPN Standard Mode - Edit Settings
Address of the remote site's VPN gateway: 192.168.10.2
Authentication method: X.509 Remote Certificate
Remote Certificate: Konfiguration-1.Gruppe1.Baugruppe2.cer
Remote ID: UA65D89FF@GE1C4
Local ID: U701515CF@GE1C4
Remote net address: 192.168.8.0
Remote subnet mask: 255.255.255.0
Local net address: 192.168.9.0
Local subnet mask: 255.255.255.0
IPSec VPN > Connections - Edit IKE
Phase 1 - ISAKMP SA
ISAKMP-SA encryption: 3DES-168
ISAKMP-SA hash: SHA-1
ISAKMP-SA mode: Main mode
ISAKMP-SA lifetime: 86400
Phase 2 - IPSec SA
IPSec-SA encryption: 3DES-168
IPSec-SA hash: SHA-1
IPSec-SA lifetime: 86400
Perfect Forward Secrecy (PFS): No
DH/PFS-group: DH-2 1024
NAT-T: On
Zeile 1, Spalte 1

– File di esportazione per unità SCALANCE M-800:


Konfiguration-1.Baugruppe1.txt - Editor
Datei Bearbeiten Format Ansicht ?
SCALANCE M-800
{
Configuration of SCALANCE M-800: Baugruppe1
Baugruppe1 in connection with Baugruppe2
Go to "System -> Load&Save -> Passwords" and store the Certificate-Password in IPSecCert row.
Go to "System -> Load&Save -> HTTP" and use IPSecCert row to upload the following files:
Konfiguration-1.U47422A8D@GB0F9.Baugruppe1.p12
Konfiguration-1.Gruppe1.Baugruppe2.cer
Go to "Security -> IPSecVPN -> Remote End"
Create a new table item with the following information:
Remote Mode: Standard
Remote Type: manual
Remote Address: Inserire l'indirizzo IP o FQDN del responder
Treat as DDNS Host Name: Attivare la casella di controllo se 'Remote Address' è un FQDN
Remote Subnet: 192.168.8.0/24
Go to "Security -> IPSecVPN -> Connections"
Create a new table item with the following information:
Keying Protocol: IKEv1
Remote End: choose the Remote End you created
Local Subnet: 192.168.9.0/24
Go to "Security -> IPSecVPN -> Authentication"
Set for your connection the following values:
Authentication: Remote Cert
Local Certificate: Konfiguration-1.U47422A8D@GB0F9.Baugruppe1_Cert.pem
Local ID: U47422A8D@GB0F9
Remote Certificate: Konfiguration-1.Gruppe1.Baugruppe2.cer
Remote ID: U6B2BC2B5@GB0F9
Zeile 1, Spalte 1

- Certificati del gruppo VPN dell'unità
  - Tipo di dati della chiave privata: File *.p12
  - Il file contiene il certificato del gruppo VPN dell'unità e il relativo materiale codificato.
  - L'accesso è protetto da password.
- Certificati CA di gruppi VPN
  - Tipo di file: File *.cer

Nota

I file di configurazione non vengono trasmessi all'unità. Viene generato un file ASCII con il quale è possibile configurare le proprietà rilevati per la VPN di SCALANCE M. A tal fine l'unità deve trovarsi almeno in un gruppo VPN con un'unità Security o un SOFTNET Security Client a partire dalla versione V3.0.

Nota

Protezione dei file di configurazione esportati da accesso non autorizzato

Dai file di configurazione esportati dal Security Configuration Tool per SCALANCE M è possibile ottenere informazioni rilevanti per la sicurezza. Per questo motivo assicurarsi che i file siano protetti da accesso non autorizzato. Questo va osservato in particolare in caso di inoltro dei file.

Generazione dei file di configurazione

1. Selezionare l'unità da modificare.
2. Selezionare la voce di menu "Trasferisci" > "Alla/alle unità...".

3. Nella finestra di salvataggio successiva indicare il percorso e il nome del file di configurazione e fare clic sul pulsante "Salva".
4. Inserire nella seguente finestra di dialogo se per il certificato dei gruppi VPN dell'unità deve essere generata una propria password.

   Se si seleziona "No", come password viene assegnato il nome della progettazione (ad es. SCALANCE_M_Konfiguration1), non la password del progetto.

   Se si seleziona "Sì" (raccomandato), è necessario inserire una password nella finestra successiva.

Risultato: I file (e i certificati) vengono salvati nella directory specificata.

Nota

Ulteriori informazioni relative alla configurazione si trovano nelle istruzioni operative delle rispettive unità SCALANCE M.

6.7 Dati di configurazione per apparecchi VPN

Significato

Le informazioni VPN per la parametrizzazione di un apparecchio VPN possono essere generate con il Security Configuration Tool. Con i file generati è quindi possibile configurare l'apparecchio VPN.

Vengono generati i seguenti file:

- File di esportazione con dati di configurazione
  - Tipo di file: File *.txt in formato ASCII
  - Contiene le informazioni di configurazione esportate per l'apparecchio VPN, compresa un'informazione su ulteriori certificati generati.

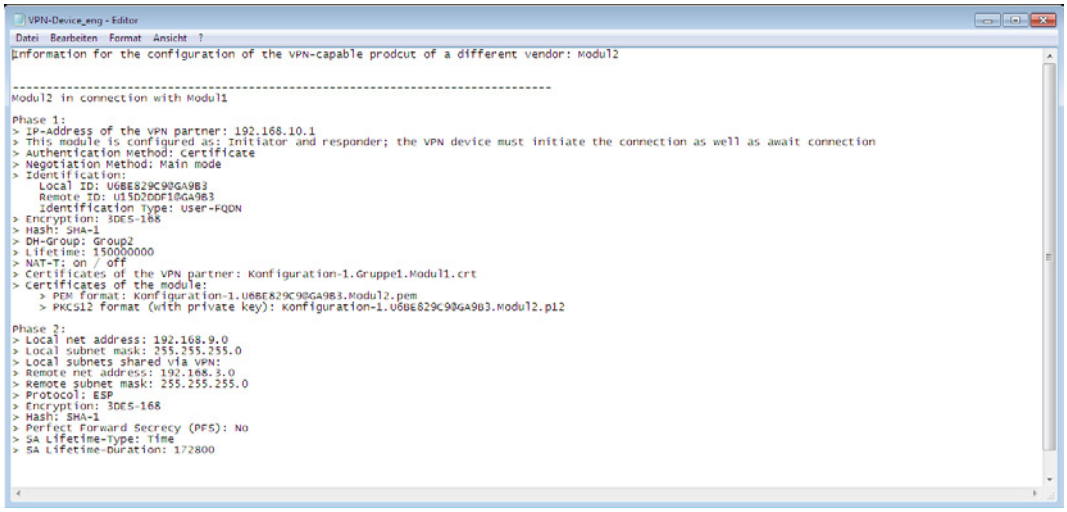

VPN-Device_eng - Editor
Datei Bearbeiten Format Ansicht ?
Information for the configuration of the VPN-capable prodcut of a different vendor: Modul2
Modul2 in connection with Modul1
Phase 1:
> IP-Address of the VPN partner: 192.168.10.1
> This module is configured as: Initiator and responder; the VPN device must initiate the connection as well as await connection
> Authentication Method: Certificate
> Negotiation Method: Main mode
> Identification:
Local ID: U6BE829C90GA9B3
Remote ID: U15D2D0F10GA9B3
Identification Type: User-FQDN
> Encryption: 3DES-168
> Hash: SHA-1
> DH-Group: Group2
> Lifetime: 150000000
> NAT-T: on / off
> Certificates of the VPN partner: Konfiguration-1.Gruppe1.Modul1.crt
> Certificates of the module:
> PEM format: Konfiguration-1.U6BE829C90GA9B3.Modul2.pem
> PKCS12 format (with private key): Konfiguration-1.U6BE829C90GA9B3.Modul2.p12
Phase 2:
> Local net address: 192.168.9.0
> Local subnet mask: 255.255.255.0
> Local subnets shared via VPN:
> Remote net address: 192.168.3.0
> Remote subnet mask: 255.255.255.0
> Protocol: ESP
> Encryption: 3DES-168
> Hash: SHA-1
> Perfect Forward Secrecy (PFS): No
> SA Lifetime-Type: Time
> SA Lifetime-Duration: 172800

Figura 6-1 File di esportazione per un dispositivo VPN

- Certificati del gruppo VPN del dispositivo VPN
- Certificati del gruppo VPN dell'unità partner
- Chiave privata
- Certificati CA di gruppi VPN

Configurazione dei tipi di file

Per i dispositivi VPN possono essere definiti i tipi di file nei quali vengono memorizzati i dati generati.

Selezionare quindi il dispositivo VPN da modificare e quindi la voce di menu "Modifica" > "Proprietà...".

- Certificati del gruppo VPN del dispositivo VPN
  - File *.crt: Certificato codificato Base64
  - File *.pem: Certificato codificato Base64
  - File *.pem: Certificato con codice binario
- Certificati del gruppo VPN dell'unità partner:
  - File *.crt: Certificato codificato Base64
  - *.pem: Certificato codificato Base64
  - *.pem: Certificato con codice binario
- Chiave privata:
  - File *.p12: Archivio PKCS12 protetto da password con chiave privata
  - *.key: Chiave provata codificata Base64 non protetta
- Certificati CA di gruppi VPN:
  - File *.crt: Certificato codificato Base64
  - File *.pem: Certificato codificato Base64
  - File *.pem: Certificato con codice binario

Nota

I file di configurazione non vengono trasmessi all'apparecchio VPN. Viene generato un file ASCII con il quale è possibile configurare l'apparecchio VPN. A tal fine l'apparecchio VPN deve trovarsi almeno in un gruppo VPN con una unità Security o un SOFTNET Security Client a partire dalla versione V3.0.

Generazione dei file di configurazione

1. Selezionare il dispositivo VPN da modificare.
2. Selezionare la voce di menu "Trasferisci" > "Alla/alle unità...".
3. Nella finestra di salvataggio successiva indicare il percorso e il nome del file di configurazione e fare clic sul pulsante "Salva".
4. Indicare nella seguente finestra di dialogo se per i due file di certificati generati deve essere creata una password propria.

   Se si seleziona "No", come password viene assegnato il nome della progettazione (ad es. VPN-Projekt_02), non la password del progetto.

   Se si seleziona "Sì" (raccomandato), è necessario inserire una password nella finestra successiva.

Risultato: I file (e i certificati) vengono salvati nella directory specificata.

6.8 Dati di configurazione per NCP VPN Client (Android)

NCP Secure VPN Client for Android

L'NCP Secure Android Client consente un collegamento VPN di elevala sicurezza a reti di dati centrali di ditte e organizzazioni. L'accesso è possibile a più reti di dati differenti con rispettivamente un proprio profilo VPN.

Sulla base dello standard IPsec i Tablet e gli Smartphone possono realizzare collegamenti di dati con gateway VPN di tutti i più noti produttori.

Il client è acquistabile in due varianti tramite il Google Play Store:

- NCP Secure VPN Client for Android (autenticazione con Preshared Key)
- NCP Secure VPN Client Premium for Android (autenticazione con Preshared Key o certificato)

Ulteriori informazioni sui client NCP Secure Android si trovano in:

NCP Secure VPN Client for Android (http://www.ncp-e.com/en/products/ipsec-vpn-client-for-android.html)

Significato

Le informazioni VPN per la parametrizzazione di un client VPN (Android) possono essere generate con il Security Configuration Tool. Con i file generati è quindi possibile configurare il software client VPN NCP.

Vengono generati i seguenti tipi di file:

- File di esportazione con dati di configurazione
  - Tipo di file: File *.ini in formato UTF 8
  - Contiene le informazioni di configurazione esportate per client VPN NCP (Android), compresa un'informazione su ulteriori certificati generati.
- Certificati del gruppo VPN dell'unità
  - Tipo di dati della chiave privata: File *.p12
  - Il file contiene il certificato del gruppo VPN dell'unità e il materiale codificato.
  - L'accesso è protetto da password.
- Certificati CA di gruppi VPN:
  - Tipo di file: File *.crt

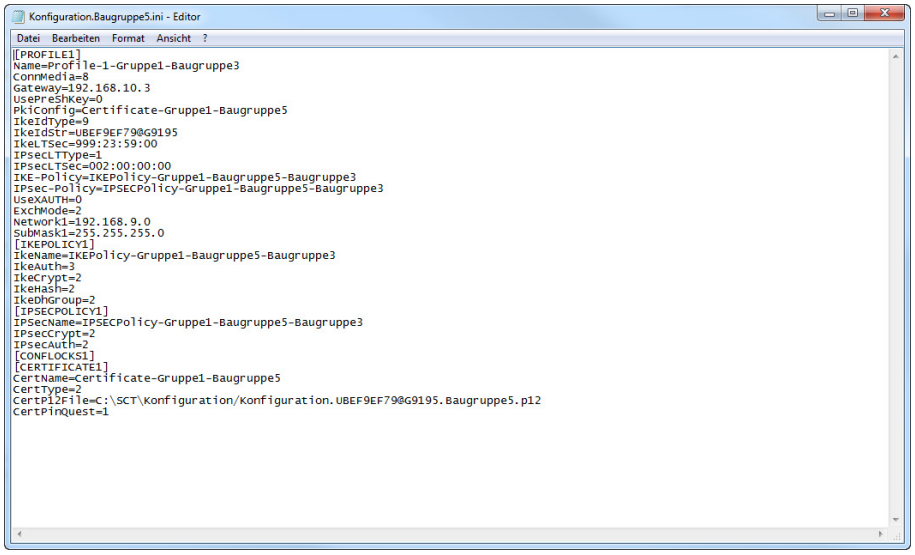


Figura 6-2 File di esportazione per un client VPN NCP (Android)

Nota

I file di configurazione non vengono trasmessi al client VPN NCP (Android). Viene generato un file ASCII con il quale è possibile configurare il client VPN NCP (Android). A tal proposito il client VPN NCP (Android) deve trovarsi almeno in un gruppo VPN con un'altra unità Security.

Generazione dei file di configurazione

1. Selezionare nell'area del contenuto il client VPN NCP (Android) da modificare.
2. Selezionare la voce di menu "Trasferisci" > "Alla/alle unità...".
3. Nella finestra di salvataggio successiva indicare il percorso e il nome del file di configurazione e fare clic sul pulsante "Salva".
4. Indicare nella seguente finestra di dialogo se per i due file di certificati generati deve essere creata una password propria.

   Se si seleziona "No", come password viene assegnato il nome della progettazione (ad es. NCP-Projekt_02), non la password del progetto.

   Se si seleziona "Sì" (raccomandato), è necessario inserire una password nella finestra successiva.

Risultato: I file vengono salvati nella directory specificata.

6.9 Configurazione di nodi di rete interni

Configurazione di nodi di rete interni

Ogni unità Security deve conoscere i nodi di rete nell'intera rete interna per poter definire l'autenticità di un telegramma.

L'unità Security deve conoscere sia i propri nodi interni sia i nodi interni delle unità Security con i quali è in un gruppo VPN. Questa informazione viene impiegata su un'unità Security per determinare quale pacchetto dati deve essere trasmesso in quale tunnel.

SCALANCE S

Oltre alla configurazione statica dei nodi di rete, un'unità SCALANCE S in modalità Bridge offre anche la possibilità di inizializzarli automaticamente.
La configurazione statica dei nodi di rete è descritta nel seguente capitolo:
Configurazione di ulteriori nodi e sottoreti per il tunnel VPN (Pagina 217)

Le informazioni relative all'apprendimento automatico di nodi interni si trovano nel seguente capitolo:
Tipo di funzionamento della modalità di programmazione (Pagina 219)

CP x43-1 Adv. e CP 1628

- CP x43-1 Adv.

  Selezionare se la comunicazione via tunnel al CP e/o alla sottorete interna per partner del collegamento VPN in modalità Routing (SCALANCE S / M / dispositivo VPN / NCP client VPN (Android)) è consentita.

- CP 1628

  Inserire i nodi NDIS che devono essere raggiungibili attraverso il tunnel dai partner del collegamento VPN in modalità Routing (SCALANCE S / M / dispositivo VPN / NCP client VPN (Android)).

6.9.1 Configurazione di ulteriori nodi e sottoreti per il tunnel VPN

Significato

Aggiungendo un'unità Security ad un gruppo VPN vengono abilitati automaticamente i nodi interni/le sottoreti locali dell'unità Security per la comunicazione via tunnel VPN. Per consentire la comunicazione tramite tunnel VPN con altre sottoreti o nodi di altre sottoreti, queste sottoreti o nodi devono essere abilitati per la comunicazione VPN tramite la configurazione.

Una sottorete che deve essere abilitata tramite la configurazione può essere:

- una sottorete raggiungibile tramite la rete locale sull'interfaccia interna, se un tunnel VPN termina sull'interfaccia esterna o sull'interfaccia DMZ.
- una sottorete raggiungibile tramite l'interfaccia DMZ, se un tunnel VPN termina sull'interfaccia esterna.
- una sottorete raggiungibile tramite l'interfaccia esterna, se un tunnel VPN termina sull'interfaccia DMZ.

Requisito richiesto

Prima che i nodi o le sottoreti possano essere abilitati per la comunicazione via tunnel devono essere soddisfatti i seguenti requisiti:

- L'unità Security si trova in un gruppo VPN.
- Il campo della finestra di dialogo "Nodi VPN" nella scheda "VPN" viene visualizzato solo se il progetto si trova in modalità estesa.

Nota

Non è possibile una ricommutazione alla modalità standard

Non appena è stata modificata la configurazione per il progetto attuale, non è più possibile annullare una commutazione nella modalità estesa precedentemente eseguita.

Rimedio SCT Standalone: chiudere il progetto senza salvarlo e aprirlo di nuovo.

A questa funzione modalità Bridge si accede nel modo seguente

Osservazione: Se i nodi o le sottoreti sull'interfaccia DMZ (solo SCALANCE S623/S627-2M) sono abilitati, seguire la descrizione per la modalità routing.

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica" > "Proprietà...", scheda "VPN".
   L'abilitazione di nodi e sottoreti si configura nel campo della finestra di dialogo "Nodi VPN".
3. Se si vogliono abilitare sottoreti complete per la comunicazione via tunnel, inserirle nella scheda "Sottorete interna". Se si vogliono abilitare singoli nodi per la comunicazione via tunnel, inserirli nella scheda "Nodi IP interni".

Osservazione: Per poter accedere alle sottoreti qui indicate, anche per queste è necessario inserire un router nella scheda "Routing". Inoltre il firewall deve consentire la comunicazione con i nodi.

A questa funzione modalità Routing si accede nel modo seguente

1. Selezionare l'unità Security da modificare.
2. Selezionare la voce di menu "Modifica" > "Proprietà...", scheda "VPN".
   L'abilitazione di sottoreti si configura nel campo della finestra di dialogo "Nodi VPN".
3. Nella scheda "Sottoreti raggiungibili via tunnel" selezionare l'ID di rete e la maschera della sottorete che deve essere inclusa nella comunicazione via tunnel.

Osservazione: Per poter accedere alle sottoreti qui indicate, anche per queste è necessario inserire un router nella scheda "Routing". Inoltre il firewall deve consentire la comunicazione con le sottoreti.

6.9.2 Tipo di funzionamento della modalità di programmazione

Ricerca automatica dei nodi per la comunicazione via tunnel (con SCALANCE S modalità Bridge)

Un grande vantaggio per la comunicazione e il funzionamento della comunicazione via tunnel consiste nel fatto che le unità SCALANCE S possono trovare autonomamente i nodi nelle reti interne. In questo modo non è necessario configurare manualmente i nodi di rete interni che devono partecipare alla comunicazione via tunnel.

I nuovi nodi vengono riconosciuti dall'unità SCALANCE S durante il funzionamento. I nodi riconosciuti vengono segnalati alle unità SCALANCE S appartenenti allo stesso gruppo. In questo modo lo scambio dei dati all'interno di un tunnel di un gruppo VPN viene garantito in qualsiasi momento in entrambe le direzioni.

Requisiti richiesti

Vengono riconosciuti i seguenti nodi:

- Nodi di rete con funzione IP

  I nodi di rete con funzione IP vengono trovati viene trasmessa una risposta ICMP al ICMP-Subnet-Broadcast.

  I nodi IP a valle dei router possono essere trovati se il router inoltra ICMP Broadcast.

- Nodi di rete ISO

  Anche i nodi di rete che non hanno funzione IP, ma che sono interrogabili tramite protocolli ISO, possono essere programmati.

  Il presupposto è che essi rispondano a telegrammi XID o TEST. TEST e XID (Exchange Identification) sono protocolli ausiliari per lo scambio di informazioni sul livello layer 2. Inviando questi telegrammi con un indirizzo Broadcast, questi nodi di rete possono essere trovati.

- Nodi PROFINET

  DCP (Discovery and basic Configuration Protocol) consente di trovare nodi PROFINET.

I nodi di rete che non soddisfano queste condizioni devono essere configurati in modo statico.

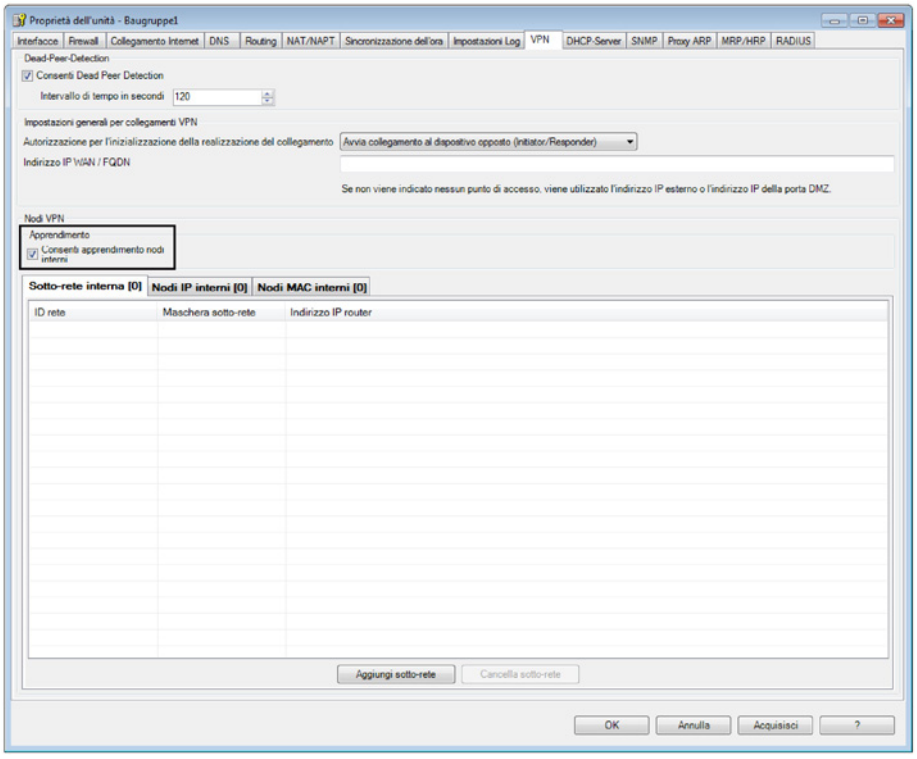
Nota

Nessuna modalità di apprendimento nel tunnel VPN sull'interfaccia DMZ S62x

L'apprendimento di nodi interni viene supportato solo sulle interfacce che vengono collegate in modalità Bridge. L'interfaccia DMZ viene già collegata in modalità routing.

Alla funzione si accede nel modo seguente

1. Selezionare l'unità SCALANCE S da modificare.
2. Selezionare la voce di menu "Modifica " > Proprietà...", scheda "VPN"



Quando è consigliabile disattivare la modalità di programmazione automatica?

Le impostazioni standard per l'unità Security presuppongono che le reti interne siano già sicure; vale a dire che anche normalmente nella rete interna non vengono attivati nodi di rete che non sono riservati.

La disattivazione della modalità di apprendimento va utilizzata se la rete interna è statica, vale a dire se il numero di nodi interni e i relativi indirizzi non si modificano.

Disattivano la modalità di programmazione, nella rete viene eliminato il carico del mezzo e dei nodi di rete dovuto ai telegrammi di programmazione. Anche le prestazioni dell'unità

SCALANCE S aumentano in quanto essa non viene caricata con l'elaborazione dei telegrammi di apprendimento.

Osservazione: nella modalità di apprendimento tutti i nodi di rete vengono registrati nella rete interna. Le indicazioni per la configurazione di VPN si riferiscono solo ai nodi di rete che comunicano nella rete interna tramite VPN.

Nota

Se nella rete interna vengono elaborati più di 128 nodi interni, viene superata la configurazione ammessa e creato uno stato di funzionamento non consentito. A causa della dinamica nel traffico di rete si verifica inoltre che i nodi interni già programmati vengano sostituiti con nuovi nodi interni finora sconosciuti.

Nodi di rete non programmabili

Nella rete interna esistono nodi che non possono essere programmati. In questo caso si tratta di nodi di sottoreti che si trovano sulla rete interna locale dell'unità SCALANCE S (ad es. router interni). Anche queste sottoreti non possono essere apprese. I nodi apprendibili e le sottoreti devono essere configurati staticamente in modalità estesa.

Nota

Non è possibile una ricommutazione alla modalità standard

Non appena è stata modificata la configurazione per il progetto attuale, non è più possibile annullare una commutazione nella modalità estesa precedentemente eseguita.
Rimedio di SCT Standalone: chiudere il progetto senza salvarlo e aprirlo di nuovo.

6.9.3 Visualizzazione dei nodi di rete interni trovati

Tutti i nodi di rete trovati vengono visualizzati nel Security Configuration Tool.

1. Passare al modo di funzionamento "Online".
2. Selezionare la voce di menu "Modifica " > Diagnostica online...", scheda "Nodi interni"

   Risultato: I nodi di rete interni trovati vengono visualizzati.

Ridondanza router e firewall 7

7.1 Informazioni generali

Significato

Grazie alla ridondanza router e firewall è possibile compensare in modo automatizzato i guasti delle unità Security SCALANCE S623 a partire da V4 e SCALANCE S627-2M a partire da V4 durante il funzionamento. Raggruppare quindi due unità Security del tipo SCALANCE S623 o SCALANCE S627-2M in una relazione di ridondanza e determinare quale deve essere l'unità Security attiva della relazione di ridondanza nel funzionamento normale. Se l'unità Security attiva si guasta, l'unità Security passiva assume automaticamente la sua funzione di firewall e router (NAT/NAPT). Per garantire una configurazione identica di entrambe le unità Security, esse vengono collegate tra loro tramite le rispettive interfacce DMZ e la relativa configurazione viene sincronizzata durante il funzionamento. In questo caso le interfacce DMZ delle unità Security coinvolte non possono essere utilizzate per altri scopi.

Ridondanza di indirizzi

Oltre ai relativi indirizzi IP dell'unità le due unità Security sull'interfaccia esterna e sull'interfaccia interna si ripartiscono rispettivamente un indirizzo IP comune in modo che in caso di guasto di una unità Security non siano necessarie modifiche di indirizzi IP. Per questo motivo per l'interfaccia esterna e per l'interfaccia interna della relazione di ridondanza è necessario progettare un indirizzo IP.

Progettazione di relazioni di ridondanza e unità Security collegate

Dopo aver collegato le unità Security ad una relazione di ridondanza, una parte delle proprietà delle unità viene progettata solo tramite la relazione di ridondanza. Questa parte delle proprietà delle unità viene disattivata per le singole unità Security ed è di nuovo attiva ed editabile dopo la rimozione delle unità Security dalla relazione di sicurezza. Le seguenti proprietà vengono progettate tramite la relazione di ridondanza:

- Impostazioni base della relazione di ridondanza (parametri di rete, unità primaria)
- Firewall
- Routing
- Routing NAT/NAPT (nessun 1:1-NAT)

Le impostazioni riportate di seguito sono attive anche dopo il collegamento in una relazione di ridondanza per le singole unità Security. Queste impostazioni possono ancora essere adattate separatamente per entrambe le unità Security.

- Impostazioni delle interfacce (la disattivazione di interfacce non è possibile)
- Regole standard per servizi IP (firewall)

- DDNS
- Sincronizzazione dell'ora
- Impostazioni Log
- SNMP
- MRP/HRP
- RADIUS

7.2 Relazioni di ridondanza e assegnazione di unità Security

Requisiti richiesti

Possono essere assegnate solo unità Security di una relazione di ridondanza che soddisfano i seguenti requisiti:

- L'unità Security è del tipo "S623 V4" o "S627-2M V4"
- L'unità Security si trova in modalità Routing
- Tutte le interfacce dell'unità Security sono attive
- Il metodo di assegnazione IP "Indirizzo statico" è progettato per tutte le interfacce
- L'unità Security non è un nodo di un gruppo VPN
- L'unità Security non è assegnata a nessuna relazione di ridondanza

Procedimento

1. Nell'area di navigazione selezionare l'oggetto "Relazione di ridondanza".
2. Selezionare nel menu contestuale (tasto destro del mouse) dell'oggetto la voce di menu "Inserisci relazione di ridondanza...".

   Risultato: La relazione di ridondanza creata viene visualizzata nell'area di navigazione.

3. Assegnare l'unità Security alla relazione di ridondanza selezionandola nell'area del contenuto e trascinandola sulla relazione di ridondanza creata nell'area di navigazione (Drag and Drop).
4. Nella finestra di dialogo "Configurazione della relazione di ridondanza" esistono le seguenti possibilità per la progettazione della relazione di ridondanza:
   - Acquisizione della progettazione dalle schede "Firewall", "Routing" e "NAT/NAPT" di un'unità Security per la relazione di ridondanza. Dalla casella di riepilogo è possibile selezionare le unità Security delle quali si intende utilizzare la progettazione per la relazione di ridondanza. Una progettazione esistente della relazione di ridondanza viene quindi sovrascritta.
   - Generazione di una copia dell'unità Security assegnata all'interno della relazione di ridondanza. Questo è possibile solo se ad una relazione di ridondanza creata viene assegnata una sola unità Security.

   In alternativa la relazione di ridondanza può essere progettata successivamente tramite le proprietà della relazione di ridondanza, vedere capitolo:
   Configurazione delle relazioni di ridondanza (Pagina 225)

Risultato: È stata creata una relazione di ridondanza e questa è stata assegnata alle unità Security desiderate.

7.3 Configurazione delle relazioni di ridondanza

A questa funzione si accede nel modo seguente

Selezionare nell'area di navigazione la relazione di ridondanza e quindi la voce di menu "Modifica" > "Proprietà...".

Progettazione dei parametri di rete della relazione di ridondanza

Tabella 7- 1 Parametri nella scheda "Impostazioni di base"

Parametro configurabile	Significato
Unità primaria	Selezione dell'unità Security che nel funzionamento normale deve essere l'unità Security attiva.
Attiva ID router virtuale (solo per SCALANCE S623/S627-2M a partire dal firmware V4.0.1)	Se si attiva questa casella di controllo, è possibile adattare le ID del router virtuali delle interfacce virtuali. Tramite una ID del router virtuale viene definito l'indirizzo MAC virtuale di un'interfaccia virtuale. Valori possibili: 01...FF
Indirizzo IP	Indirizzo IP virtuale dell'interfaccia esterna o interna della relazione di ridondanza
Maschera della sottorete	Maschera della sottorete dell'interfaccia virtuale esterna o interna della relazione di ridondanza

Parametro configurabile	Significato
Commento	Commento opzionale
ID router virtuale (solo per SCALANCE S623/S627-2M a partire dal firmware V4.0.1)	Tramite una ID del router virtuale viene definito l'indirizzo MAC virtuale di un'interfaccia virtuale.

Per informazioni generali sulla progettazione dei parametri di rete vedere il seguente capitolo:
Creazione di unità e impostazione dei parametri di rete (Pagina 85)

Progettazione del firewall

La progettazione delle regole del filtro pacchetto IP per le relazioni di ridondanza viene eseguita in base allo stesso schema della progettazione delle regole filtro pacchetto IP per le singole unità Security. Sono a disposizione le direzioni di comunicazione "Dall'esterno all'interno" e " Dall'interno all'esterno".

Per informazioni generali sulla progettazione delle regole filtro pacchetto IP in modalità estesa vedere il seguente capitolo:
Regole del filtro pacchetto IP (Pagina 145)

Progettazione della conversione di indirizzi con NAT/NAPT

La progettazione della conversione di indirizzi con NAT/NAPT per la relazione di ridondanza viene eseguita in base allo stesso schema della progettazione della conversione di indirizzi con NAT/NAPT per le singole unità Security. Per le relazioni di ridondanza può essere progettato solo Source NAT e NAPT. In Source NAT gli indirizzi IP sorgente nella sottorete interna possono essere scambiati solo con indirizzi IP virtuali esterni della rete di ridondanza. Non possono essere registrati indirizzi IP Alias sull'interfaccia esterna della relazione di ridondanza. In NAPT è progettabile solo la direzione di conversione di indirizzi "Da esterno a interno".

Per informazioni generali sulla progettazione delle conversioni di indirizzi con NAT/NAPT vedere il seguente capitolo:
Conversione di indirizzi NAT/NAPT (Pagina 168)

Progettazione del routing

La progettazione degli instradamenti per la relazione di ridondanza viene eseguita in base allo stesso schema della progettazione degli instradamenti per le singole unità Security.

Per informazioni generali sulla progettazione di routing vedere il seguente capitolo:
Definizione del router standard e degli instradamenti (Pagina 164)

Vedere anche

Regole del filtro pacchetto MAC (Pagina 155)

SOFTNET Security Client

8

Con il software PC SOFTNET Security Client sono possibili accessi remoti sicuri dal PC/PG agli apparecchi di automazione protetti da unità Security, in tutte le reti pubbliche.

Questo capitolo descrive come eseguire la progettazione del SOFTNET Security Client nel Security Configuration Tool e la successiva messa in servizio sul PC/PG.

Altre informazioni

Le informazioni dettagliate sulle finestre di dialogo e i parametri impostabili si trovano anche nella guida in linea del SOFTNET Security Client.

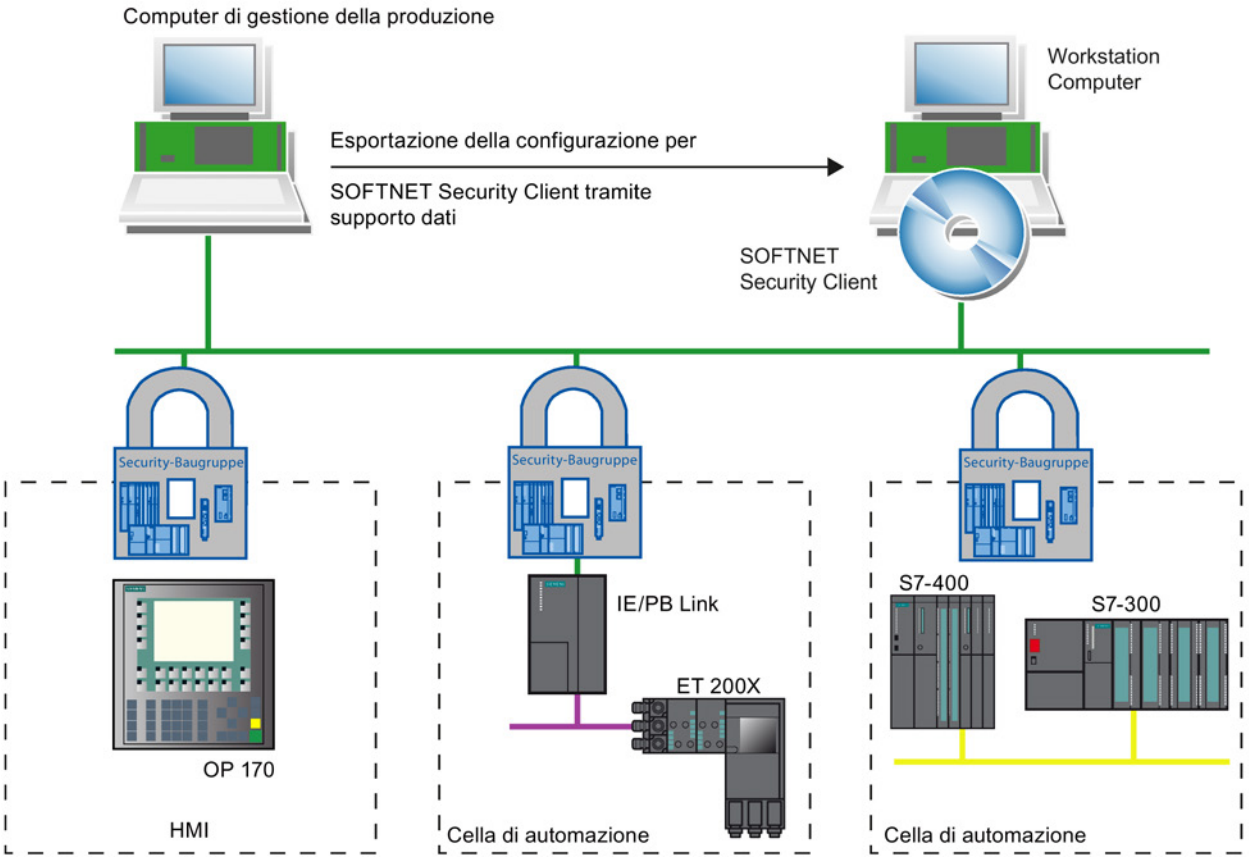
Alla guida è possibile accedere con il tasto F1 o con il pulsante "Help" nella relativa finestra di dialogo.

8.1 Impiego del SOFTNET Security Client

Campo d'impiego - Accesso tramite VPN

Con il SOFTNET Security Client configurare un PC/PG in modo che esso possa realizzare un collegamento via tunnel IPsec protetto nella VPN (Virtual Private Network) con una o diverse unità Security.

Le applicazioni PG/PC come la diagnostica NCM o STEP7 possono accedere con un collegamento via tunnel protetto ad apparecchi o reti che si trovano in una rete interna protetta con l'unità Security.



Comunicazione automatica tramite VPN

Per la propria applicazione è importante che il SOFTNET Security Client riconosca se avviene l'accesso agli indirizzi IP di un nodo VPN. Indirizzare il nodo tramite l'indirizzo IP come se si trovasse nella sotto-rete locale alla quale è collegato anche il PC/PG con applicazioni.

Nota

Tramite il tunnel IPsec può essere eseguita solo una comunicazione basata su IP tra SOFTNET Security Client e le unità Security, nonché i nodi interni dopo le unità Security. La comunicazione livello 2 non è possibile con il SOFTNET Security Client.

Dettagli nella guida in linea

Le informazioni dettagliate sulle finestre di dialogo e le caselle di immissione si trovano anche nella guida in linea della superficie operativa del SOFTNET Security Client.

La guida in linea si richiama con il pulsante "Help" o premendo il tasto F1.

Come funziona il SOFTNET Security Client?

Nella prima fase si crea con il file di configurazione per SOFTNET Security Client con Security Configuration Tool o con STEP 7 V12 o superiore.

SOFTNET Security Client legge la configurazione creata e rileva dal file i certificati da importare.

Il certificato Root e la chiave privata importati e memorizzati nel PG/PC locale.

Successivamente con i dati della configurazione vengono eseguite le impostazioni Security in modo che le applicazioni possano accedere ai servizi sulle e dopo le unità Security tramite gli indirizzi IP.

Se la modalità di programmazione è attivata per i nodi o i dispositivi di automazione interni, l'unità di configurazione imposta dapprima una direttiva di sicurezza per l'accesso protetto alle unità Security. Successivamente il SOFTNET Security Client rileva gli indirizzi IP dei rispettivi nodi interni e li inserisce in elenchi di filtri specifici della direttiva di sicurezza. Le direttive di sicurezza dei nodi interni reinizializzati devono essere attivate manualmente.

Risultato: Le applicazioni, quali ad es es. STEP 7, comunicare con gli apparecchi di automazione tramite VPN.

Sistemi operativi supportati

Il SOFTNET Security Client è adatto per l'impiego nei seguenti sistemi operativi:

- Microsoft Windows 7 a 32/64 bit + Service Pack 1
- Microsoft Windows Server 2012 R2

Se si impiega Microsoft Windows XP, utilizzare una versione precedente di SSC, ad es. SSC V4.0 per Windows XP a 32 bit + Service Pack 3.

Comportamento in caso di disturbi

Al verificarsi di disturbi sul proprio PG/PC, il SOFTNET Security Client presenta il seguente comportamento:

- Le direttive di sicurezza configurate vengono mantenute tramite disinserimento e inserimento del proprio PG/PC;
- In caso di configurazione errata vengono emessi messaggi.

8.2 Installazione del SOFTNET Security Client

8.2.1 Installazione del SOFTNET Security Client

Regola generale

Il software PC SOFTNET Security Client si installa dal DVD del prodotto.

1. Leggere dapprima le indicazioni riportate nel file README del DVD SCALANCE S e osservare eventuali istruzioni di installazione supplementari.
2. Eseguire il programma di setup;

   Aprire quindi il sommario del contenuto sul DVD SCALANCE S CD → viene avviato automaticamente inserendo il DVD o può essere aperto con il file start.exe. Selezionare direttamente la voce "Installation SOFTNET Security Client"

ATTENZIONE
Incompatibilità con altri software client VPN
Se nel PC oltre al SOFTNET Security Client è installato un altro software client VPN, con il SOFTNET Security Client non può eventualmente più essere realizzato nessun tunnel VPN. Per questo motivo disinstallare dapprima questo software client VPN prima di utilizzare il client SOFTNET Security.

Comportamento all'avvio

Il caricamento delle regole di sicurezze può durante un certo periodo. In questo tempo la CPU del PG/PC viene occupata fino al 100%

8.2.2 Disinstallazione del SOFTNET Security Client

Durante la disinstallazione vengono ripristinate le proprietà Security impostate dal SOFTNET Security Client.

8.3 Impostazione dei file di configurazione con lo strumento di progettazione Security Configuration Tool

Configurazione del SOFTNET Security Client nel progetto SCT

Il SOFTNET Security Client viene creato nel progetto SCT come unità. Rispetto alle altre unità Security non devono essere progettate altre proprietà.

Assegnare il SOFTNET Security Client creato o i gruppi VPN nei quali deve essere configurato il tunnel IPsec con il PC/PG. In questo caso vengono acquisite le proprietà dei gruppi progettate per questi gruppi VPN.

Nota

Osservare le indicazioni relative ai parametri nel seguente capitolo:

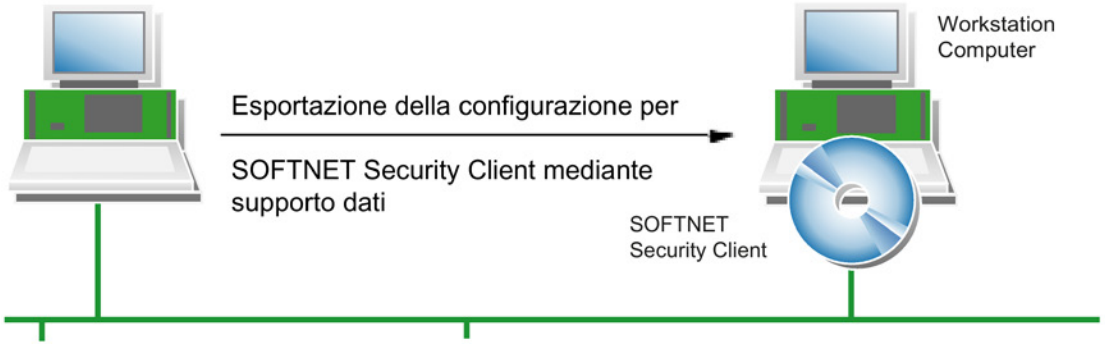
- Acquisizione dell'unità nel gruppo VPN configurato (Pagina 202)

Nota

Se si creano più SOFTNET Security Client all'interno di un gruppo non vengono realizzati tunnel tra questi client, ma solo dal relativo client alle unità Security!

File di configurazione per il SOFTNET Security Client

L'interfaccia tra lo strumento di progettazione Security Configuration Tool e il SOFTNET Security Client viene comandata con i file di configurazione.



La configurazione viene memorizzata nei seguenti tipi di file:

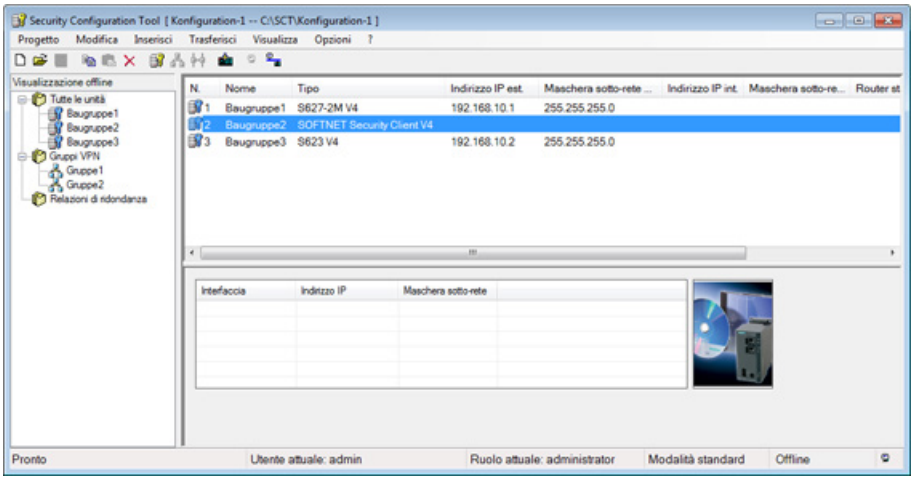
- *.dat
- *.p12
- *.cer

Procedimento

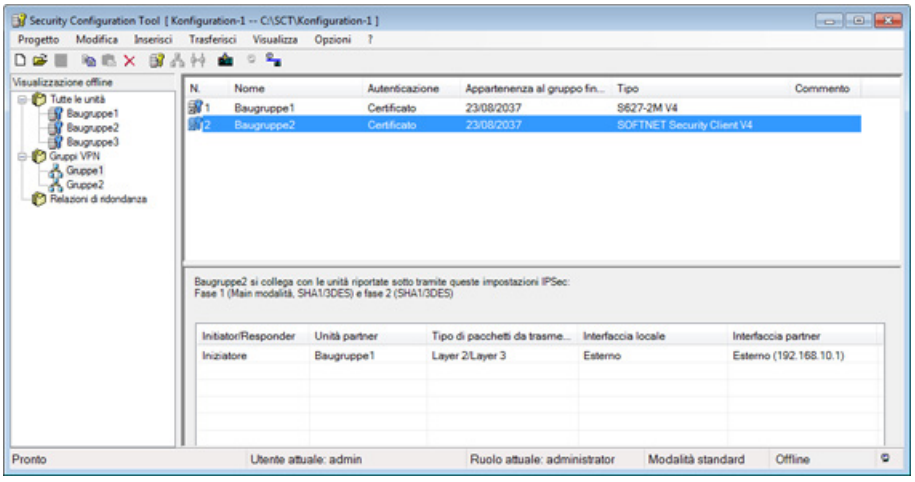
Per generare i file di configurazione eseguire le seguenti operazioni in SCT:

1. Creare in SCT un'unità del tipo client SOFTNET Security.

   Osservazione: se si seleziona la release del firmware "V4" per il SOFTNET Security Client, si dispone dell'insieme completo delle funzioni di SOFTNET Security Client V4 e V5.



2. Assegnare l'unità SSC ai gruppi VPN nei quali il PG/PC deve comunicare tramite tunnel IPsec.


Security Configuration Tool [Konfiguration-1 -- C:\SCT\Konfiguration-1]
Progetto Modifica Inserisci Trasferisci Visualizza Opzioni ?
Visualizzazione offline
Tutte le unità
Baugruppe1
Baugruppe2
Baugruppe3
Gruppi VPN
Gruppe1
Gruppe2
Relazioni di ridondanza
N. Nome Autenticazione Appartenenza al gruppo fin... Tipo Commento
1 Baugruppe1 Certificato 23/08/2037 S627-2M V4
2 Baugruppe2 Certificato 23/08/2037 SOFTNET Security Client V4
Baugruppe2 si collega con le unità riportate sotto tramite queste impostazioni IPSec:
Fase 1 (Main modalità, SHA1/3DES) e fase 2 (SHA1/3DES)
Initiator/Responder Unità partner Tipo di pacchetti da trasme... Interfaccia locale Interfaccia partner
Iniziatore Baugruppe1 Layer 2/Layer 3 Esterno Esterno (192.168.10.1)
Pronto
Utente attuale: admin
Ruolo attuale: administrator
Modalità standard
Offline

3. Selezionare la voce di menu "Progetto" > "Salva".
4. Selezionare l'unità del tipo "SOFTNET Security Client" e successivamente la voce di menu "Trasferisci" > "Alla/alle unità...".
5. Selezionare la posizione di memorizzazione per i file di configurazione.

6. Inserire nella seguente finestra di dialogo se per il certificato dei gruppi VPN dell'unità deve essere generata una propria password.

   Se si seleziona "No", come password viene assegnato il nome della progettazione (ad es. SCALANCE_SSC_Konfiguration1), non la password del progetto.

   Se si seleziona "Sì" (raccomandato), è necessario inserire una password nella finestra successiva.

7. Trasferire i file del tipo *.dat, *.p12, *.cer nel PG/PC nel quale si intende utilizzare il client SOFTNET Security. I file del tipo *.p12 sono disponibili se nel Security Configuration Tool come metodo di autenticazione è stato selezionato "Certificato".

8.4 Finestra di dialogo principale del SOFTNET Security Client

Proprietà configurabili

In particolare si possono utilizzare i seguenti servizi:

- Configurazione della comunicazione via tunnel IPsec protetta (VPN) tra il PC/PG e tutte le unità Security di un progetto o delle singole unità Security. Tramite questo tunnel IPSec il PC/PG può accedere alle unità Security e ai relativi nodi interni.
- Disattivazione e attivazione di collegamenti sicuri già configurati.
- Possibile solo con il modulo di apprendimento attivato: Configurare i collegamenti nei terminali di dati aggiunti in seguito.
- Controllo di una configurazione, vale a dire quali collegamenti sono configurati o possibili.

Tabella 8- 1 Caselle di visualizzazione / opzioni della finestra principale

Casella di visualizzazione / opzione	Significato
Started with user	Il nome utente con i cui dati di login è stato avviato il SOFTNET Security Client. Questi dati di login determinano la configurazione del SOFTNET Security Client che viene richiamata. Se il nome utente dell'utente che ha avvitato SOFTNET Security Client è diverso dall'utente che ha eseguito il login in Windows, il nome utente visualizzato viene contrassegnato in rosso.
Managed configuration	La configurazione richiamata per un utente o un gruppo viene visualizzata nel campo "Managed configuration". Ciascuna impostazione eseguita nel SOFTNET Security Client viene acquisita quindi automaticamente in questa configurazione. Nella casella "Type" viene indicato se per configurazione gestita si tratta di una configurazione singola o di una configurazione di gruppo. La configurazione gestita può essere modificata solo da utenti privilegiati nella finestra di dialogo "Manage users and groups". A questa finestra di dialogo si accede tramite la voce di menu "Users/Groups > Manage users and groups". Informazioni dettagliate sui privilegi della configurazione nel SOFTNET Security Client si trovano nel capitolo Creazione della configurazione gestita - Finestra di dialogo "Manage users and groups" (Pagina 239)

Casella di visualizzazione / opzione	Significato
SOFTNET Security client status	• Service: Indica se il servizio SOFTNET Security Client è in corso. • License: Indica lo stato della licenza del SOFTNET Security Client. • Privileges: Indica se l'utente, con dati di login del quale è stato avviato il SOFTNET Security Client, dispone attualmente dei diritti per caricare i dati di configurazione VPN per il SOFTNET Security Client o per le impostazioni SOFTNET Security Client avanzate. Se in linea di principio l'utente dispone di questi diritti, ma non ha avviato il SOFTNET Security Client come amministratore, l'utente può aumentare i suoi privilegi tramite il pulsante "Increase". Le informazioni dettagliate relative ai privilegi della configurazione nel SOFTNET Security Client si trovano nel capitolo Creazione della configurazione gestita - Finestra di dialogo "Manage users and groups" (Pagina 239)
Minimize	Riduce a icona la superficie operativa di SOFTNET Security Client. L'icona di SOFTNET Security Client rimane visibile nella barra delle applicazioni di Windows.
Exit	Chiude la superficie operativa del SOFTNET Security Client. Se nelle impostazioni di SOFTNET Security Client è attiva l'opzione "Limited", vengono inoltre interrotti tutti i collegamenti tramite tunnel VPN attivi.

Se SOFTNET Security Client viene avviato da un altro utente con diritti di amministratore, l'area "VPN Control" visualizza le seguenti opzioni.

Tabella 8- 2 Opzioni nella finestra di dialogo "VPN control"

Opzione	Significato
Load Configuration	Con questo pulsante si apre una finestra di dialogo per la selezione del file di configurazione creato con il Security Configuration Tool.
Disable / Enable	Disattiva / attiva tutti i tunnel protetti.
Tunnel Overview	Finestra di dialogo per la configurazione e la diagnostica del tunnel. In questa finestra di dialogo si trova un elenco dei tunnel protetti configurati.

Se SOFTNET Security Client viene avviato da un altro utente senza diritti di amministratore, l'area "VPN Diagnostics" visualizza solo il pulsante "Tunnel Overview".

ATTENZIONE
Incompatibilità con altri software client VPN Se nel PC oltre al SOFTNET Security Client è installato un altro software client VPN, con il SOFTNET Security Client non può eventualmente più essere realizzato nessun tunnel VPN. Per questo motivo disinstallare dapprima questo software client VPN prima di utilizzare il client SOFTNET Security.

8.5 Caricamento del file di configurazione e configurazione dei collegamenti via tunnel

Di seguito si trova una panoramica della configurazione dei collegamenti via tunnel. Seguendo questi passi si attraversano diverse finestre di dialogo per le quali possono essere richiamate altre informazioni in modo mirato tramite il tasto F1.

Presupposto

Il SOFTNET Security Client è stati avviato con diritti amministrativi.

Procedimento

1. Aprire con il pulsante "Load Configuration..." la finestra di dialogo per l'importazione dei file di configurazione.
2. Selezionare il file di configurazione creato con il Security Configuration Tool.
3. Se nel SOFTNET Security Client esistono già dati di configurazione viene richiesto di decidere il trattamento dei file di configurazione nuovi da assumere. Se i collegamenti via tunnel VPN devono essere realizzati con tutti i nodi interni dell'unità Security, attivare la casella di controllo "Establish VPN tunnel to the internal nodes". Se l'attivazione non viene ancora avviata in questa finestra, è possibile avviarla successivamente nella panoramica del tunnel.
4. Selezionare event. l'adattatore di rete dall'indirizzo IP del quale devono essere realizzati i collegamenti via tunnel VPN. Nella panoramica del tunnel è possibile eseguire questa impostazione in modo specifico per l'unità tramite il menu contestuale di un'unità.
5. Se durante la configurazione nel Security Configuration Tool come metodo di autenticazione è stato selezionato il certificato, viene richiesto di inserire anche la password.
6. Se durante la configurazione nel Security Configuration Tool è stata progettata un'unità SCALANCE M875, un'unità SCALANCE M-800 o un CP S7 con DHCP attivato sull'interfaccia GBit, compare la finestra di dialogo "DNS/IP settings". In base al tipo di unità progettato procedere nel modo seguente:
   - Per unità SCALANCE M875 e unità SCALANCE M-800: Selezionare se si intente realizzare il tunnel verso l'unità tramite l'indirizzo IP rilevato da ISP durante il tempo di esecuzione o alternativamente tramite un altro nome DNS.
   - Per CP S7 con DHCP attivato sull'interfaccia GBit: Inserire l'indirizzo IP assegnato tramite DHCP.

   Nota

   Impostazione del firewall in Windows 7

   Se in Windows 7 viene richiesto in che rete si intende autorizzare la comunicazione del SOFTNET Security Client, è necessario autorizzare la comunicazione del SOFTNET Security Client nelle reti pubbliche in quanto il SOFTNET Security Client altrimenti non visualizza i nodi appresi nella panoramica del tunnel.

7. Richiamare quindi la finestra di dialogo "Tunnel Overview" nella finestra di dialogo principale con il pulsante "Tunnel Overview".
   Nella tabella visualizzata si trovano le unità Security e i nodi con le informazioni di stato sui collegamenti via tunnel.

Vedere anche

Creazione della configurazione gestita - Finestra di dialogo "Manage users and groups" (Pagina 239)

8.6 Diagnostica e configurazione del tunnel - finestra di dialogo "Tunnel Overview"

Significato

Nella tabella visualizzata si possono vedere le unità e i nodi con le informazioni di stato sui collegamenti via tunnel.

Pulsante "Delete"

Con questo pulsante si cancellano tutte le direttive di sicurezza IP configurate attraverso il SOFTNET Security Client.

Selezione e comando della voce tunnel

È possibile selezionare una voce e utilizzare le seguenti voci di menu del menu contestuale:

Voce di menu	Significato
Enable all Members (Attiva collegamento con nodi interni) / Disable all Members (Disattiva collegamento con nodi interni)	I collegamenti via tunnel configurati vengono interrotti con la voce "Disable all Members". Risultato: L'icona nella colonna "Status" della panoramica dei tunnel viene sostituita. Sul PC è disattivata la direttiva di sicurezza. Per annullare la modifica e riattivare i tunnel configurati fare clic sulla voce "Enable all Members ".
Select Network Device...	Se nel proprio PC si utilizzano diverse schede di rete, con questo comando è possibile selezionare la scheda di rete tramite la quale è raggiungibile il nodo selezionato.
Reachability test	Viene inviato un comando ping all'unità selezionata.
Extended Diagnostics	Viene richiamata la finestra di dialogo "Extended Diagnostics". In questa finestra di dialogo è selezionata l'unità selezionata nella panoramica del tunnel.
Delete Entry	La direttiva di sicurezza IP della voce selezionata viene cancellata.

Nota

Estensione della direttiva di sicurezza durante l'attivazione di nodi interni

Fare attenzione che in caso di singole attivazioni del nodo interno la direttiva di sicurezza nel sistema viene rispettivamente estesa. Una disattivazione dell'intero sistema (tramite il menu contestuale dello SCALANCE S sovraordinato) non comporta tuttavia un adattamento della direttiva di sicurezza, ma solo la sua disattivazione. In questo modo in caso di attivazione di un nodo interno viene attivata sempre la direttiva generale di sicurezza più il nodo interno. Se si vuole essere sicuri che la direttiva di sicurezza configurata si riferisca completamente ad un nodo attivato, chiudere il SOFTNET Security Client e aprirlo di nuovo.

Riconoscimento di nodi previsti, non visualizzati

Se si constata che i nodi desiderati non vengono visualizzati nella tabella, procedere nel modo seguente:

Trasferire nella riga di comando un comando Ping sul nodo desiderato.

In questo modo si consente che il nodo venga appreso dall'unità Security e inoltrato al SOFTNET Security Client. Se esso non viene appreso, è necessario configurare i nodi in modo statico nella scheda VPN del Security Configuration Tool.

Nota

Nodi e sotto-reti configurati staticamente

Se si configurano in seguito staticamente nodi o sotto-reti, è necessario ricaricare anche la configurazione per un SOFTNET Security Client utilizzato nel gruppo VPN.

Parametri

Parametri	Significato / Campo dei valori
Status	Il significato delle indicazioni di stato sono riportate nella seguente tabella.
Name	Nome dell'unità o del nodo acquisito dal file di configurazione del Security Configuration Tool.
Member IP / Subnet	Se esistono nodi interni / sotto-reti interne, viene visualizzato l'indirizzo IP del nodo interno o dell'ID rete della sotto-rete interna
Tunnel Endpoint IP	Indirizzo IP dell'unità Security assegnata.
Tunnel over	Indirizzo IP della scheda di rete del proprio PC dal quale viene realizzato il tunnel VPN.

Tabella 8- 3 **Informazioni sullo stato***

Simbolo	Significato
	Non esiste nessun collegamento con l'unità o il nodo.
	Esistono altri nodi che non vengono visualizzati. Fare doppio clic sull'icona per visualizzare altri nodi.
	Il tunnel al nodo è disattivato. Nel sistema non è configurata nessuna direttiva di sicurezza IP. La comunicazione con questo nodo non è codificata.
	Il tunnel al nodo è attivato. Nel sistema è configurata una direttiva di sicurezza IP. La comunicazione è codificata e quindi protetta con questo nodo.
	Il tunnel all'unità SCALANCE S è disattivato. Nel sistema non è configurata nessuna direttiva di sicurezza IP. La comunicazione con questa unità non è codificata.
	Il tunnel all'unità SCALANCE S è attivato. Nel sistema è configurata una direttiva di sicurezza IP. La comunicazione è codificata e quindi protetta con questa unità.
	Il tunnel all'unità SCALANCE M875/M-800 è disattivato. Nel sistema non è configurata nessuna direttiva di sicurezza IP. La comunicazione con questa unità non è codificata.
	Il tunnel all'unità SCALANCE M875/M-800 è attivo. Nel sistema è configurata una direttiva di sicurezza IP. La comunicazione è codificata e quindi protetta con questa unità.
	Il tunnel al modulo CP343-1 Advanced è disattivato. Nel sistema non è configurata nessuna direttiva di sicurezza IP. La comunicazione con questo CP non è codificata.
	Il tunnel al modulo CP343-1 Advanced è attivato. Nel sistema è configurata una direttiva di sicurezza IP. La comunicazione è codificata e quindi protetta con questo CP.
	Il tunnel al modulo CP443-1 Advanced è disattivato. Nel sistema non è configurata nessuna direttiva di sicurezza IP. La comunicazione con questo CP non è codificata.
	Il tunnel al modulo CP443-1 Advanced è attivato. Nel sistema è configurata una direttiva di sicurezza IP. La comunicazione è codificata e quindi protetta con questo CP.
	Il tunnel ai CP1628 / CP 1243-1 / CP 1543-1 è disattivato. Nel sistema non è configurata nessuna direttiva di sicurezza IP. La comunicazione con questo CP non è codificata. Osservazione: i file di configurazione per SOFTNET Security Client con cui si definiscono i tunnel VPN ai CP 1243-1 e CP 1543-1 possono essere creati con STEP 7 a partire dalla versione V12 SP1.
	Il tunnel ai CP1628 / CP 1243-1 / CP 1543-1 è attivo. Nel sistema è configurata una direttiva di sicurezza IP. La comunicazione è codificata e quindi protetta con questo CP. i file di configurazione per SOFTNET Security Client con cui si definiscono i tunnel VPN ai CP 1243-1 e CP 1543-1 possono essere creati con STEP 7 a partire dalla versione V12 SP1.
	Il tunnel alla sottorete interna è disattivato. Nel sistema non è configurata nessuna direttiva di sicurezza IP.
	Il tunnel alla sottorete interna è attivato. Nel sistema è configurata una direttiva di sicurezza IP.
	L'unità / il nodo non è raggiungibile.
	L'unità / il nodo è raggiungibile, il tunnel all'unità / al nodo è tuttavia disattivato. Nel sistema non è configurata nessuna direttiva di sicurezza IP. La comunicazione con questa unità / con questo nodo non è codificata.
	L'unità / il nodo è raggiungibile, il tunnel all'unità / al nodo è attivo.
	Test di raggiungibilità disattivato. Non è possibile fare una dichiarazione sulla raggiungibilità del nodo.

* In Windows 7 SP1 e versioni successive è valida la tabella con il firewall Windows attivato.

Consolle logging

Le voci che vengono visualizzate nella consolle Log vanno selezionate nella finestra di dialogo "Impostazioni". A questa finestra di dialogo si accede nella finestra di dialogo principale del SOFTNET Security Client con la voce di menu "Settings" > "SOFTNET Security Client settings".

Vengono visualizzate le seguenti informazioni:

- Le informazioni di diagnostica per la realizzazione del collegamento con le unità Security e i nodi interni / le sotto-reti interne configurati.
- Data e ora al momento degli eventi
- Realizzazione e interruzione di una direttiva di sicurezza
- Test di raggiungibilità eseguito negativamente (ping test) con i nodi configurati
- Download configuration files
- Attiva/disattiva Learn internal nodes/subnets

Ulteriori avvertenze

- I nodi inseriti nell'elenco ma non più presenti nella sottorete restano nell'elenco per un determinato periodo (ca. 10 minuti); entro questo periodo viene controllato se è ancora possibile accedere al nodo. Se il nodo non è più raggiungibile, la voce viene cancellata dall'elenco e comprare una voce corrispondente nella consolle Log.

8.7 Creazione della configurazione gestita - Finestra di dialogo "Manage users and groups"

Utenti privilegiati /non privilegiati

In SOFTNET Security Client si distingue tra utenti privilegiati e non privilegiati. Gli utenti privilegiati sono quelli che dispongono di diritti di amministratore in Windows.

Utenti privilegiati

Gli utenti privilegiati possono eseguire tutte le impostazioni nel SOFTNET Security Client, caricare i file di configurazione VPN e diagnosticare i tunnel VPN nella panoramica dei tunnel.

La finestra di dialogo "Manage users and groups" offre agli utenti privilegiati la possibilità di creare configurazioni per utenti non privilegiati, attive automaticamente dopo il login di questo utente in Windows. In questo modo anche gli utenti non privilegiati possono utilizzare collegamenti via tunnel VPN.

Gli utenti privilegiati possono inoltre raggruppare utenti in gruppi e creare quindi le configurazioni dei gruppi VPN per questi gruppi. In questo modo è possibile ridurre il tempo di configurazione.

Utenti non privilegiati

Gli utenti non privilegiati hanno solo diritti limitati per la configurazione del SOFTNET Security Client e non possono caricare i file di configurazione VPN. Tra i diritti di utenti non privilegiati vi sono:

- l'utilizzo del tunnel VPN e la diagnostica dello stato della panoramica dei tunnel
- l'attivazione/la disattivazione del tunnel VPN nella finestra di dialogo principale
- l'attivazione del collegamento ai nodi interni appresi nella panoramica dei tunnel
- esecuzione di impostazioni per la consolle Log e per la lingua nella finestra di dialogo "Settings"
- accesso alle informazioni di diagnostica della finestra di dialogo "Extended Diagnostics" e "Log files"

Finestra di dialogo "Currently managed configuration"

In questa finestra viene visualizzato il nome e il tipo della configurazione attualmente gestita. Questa configurazione può essere modificata nella finestra di dialogo visualizzata.

Finestra di dialogo "VPN group configurations"

In questa finestra creare gruppi ai quali possono essere assegnati utenti. Un gruppo creato viene attivato per la gestione tramite il pulsante "Edit" e quindi visualizzato nella finestra di dialogo "Currently managed configuration". Ciascuna modifica eseguita di seguito nel SOFTNET Security Client viene acquisita automaticamente in questa configurazione del gruppo. Durante il login di un utente di questo gruppo in Windows viene richiamata automaticamente la configurazione del gruppo. Per ogni gruppo viene visualizzato il numero di dispositivi della configurazione corrispondente e il file di configurazione caricato per ultimo.

Nota

Modifica delle configurazioni dei gruppi

Se un utente con diritti amministrativi esegue modifiche in una configurazione del gruppo VPN, le modifiche si ripercuotono su tutti i nodi di questo gruppo.

Finestra di dialogo "VPN single configurations"

In questa finestra vengono visualizzati tutti gli utenti che hanno effettuato almeno un login in Windows e che quindi sono diventati riconoscibili per il SOFTNET Security Client. Per questi utenti la gestione può essere attivata tramite il pulsante "Edit". La configurazione viene successivamente visualizzata nella finestra di dialogo "Currently managed configuration". Ciascuna modifica eseguita di seguito nel SOFTNET Security Client viene acquisita automaticamente in questa configurazione singola. Durante il login dell'utente in Windows viene richiamata automaticamente la configurazione singola. Per ogni utente viene visualizzato il numero di dispositivi della configurazione corrispondente e il file di configurazione caricato per ultimo.

Alla voce "User accounts unknown to the SOFTNET Security Client" vengono raggruppati tutti gli utenti creati in Windows che tuttavia non hanno ancora eseguito un login.

8.8 Esecuzione della diagnostica estesa - finestra di dialogo "Extended Diagnostics"

Apertura della diagnostica estesa

Selezionare nella finestra principale del SOFTNET Security Client la voce di menu "Diagnostics" > "Extended Diagnostics". In alternativa la diagnostica può essere richiamata tramite il menu contestuali di una voce nella panoramica dei tunnel.

Nella diagnostica estesa è possibile rilevare lo stato attuale del proprio sistema in relazione ad un'unità configurata. Questa panoramica serve alla diagnostica dello stato del sistema e può essere d'aiuto in caso di richieste da parte del Customer Support.

- Module Specific Parameters (parametri specifici per l'unità)
  Qui si seleziona l'unità della quale si vuole diagnosticare lo stato attuale del sistema.
- Route Settings (Module Specific Parameters)
  Qui vengono visualizzate le impostazioni dell'unità rilevate dalla configurazione, riguardanti le interfacce e i nodi interni / le sottoreti.
- Active Main Modes / Active Quick Modes
  Qui vengono visualizzate dettagliatamente le modalità principali e le modalità rapide non appena esse sono state configurate per l'unità selezionata sul PG/PC.
  Inoltre viene visualizzato quante modalità principali e modalità rapide inerenti all'unità selezionata sono state trovate nel sistema.
- Route Settings (Host Network Settings)
  Qui vengono visualizzate le impostazioni attuali di routing del computer.
  Per motivi di chiarezza, con l'opzione "Show entire Routing Table" è possibile mostrare le impostazioni routing nascoste.
- Assigned IP Addresses
  Qui viene visualizzato un elenco sulle interfacce di rete conosciute sul computer in combinazione con gli indirizzi IP configurati e assegnati.

8.9 Accesso ai file Log - finestra di dialogo "Log files"

Accesso ai file Log

Selezionare nella finestra principale del SOFTNET Security Client la voce di menu "Diagnostics" > "Log files".

In questa finestra di dialogo si accede a tutti i file Log del SOFTNET Security Client.

È possibile:

- Aggiornare l'anteprima della finestra di segnalazione del file Log selezionato.
- Far scorrere automaticamente verso il basso il contenuto della finestra di segnalazione.
- Salvare il file Log in un editor di testo.
- Accedere alle cartelle nelle quali vengono salvati i file Log.

Le funzioni possibili sono riportate nella seguente tabella.

Funzione	Descrizione / Opzioni
SOFTNET Security Client service: General log file	Informazioni sull'avvio e la chiusura del SOFTNET Security Client. Il file Log contiene ad es. informazioni per l'avvio del SOFTNET Security Client per il controllo della licenza e per il caricamento dei dati di configurazione. Interazione del SOFTNET Security Client con l'utente e le unità Security: Riconoscimento del nuovo dispositivi, attivazione/disattivazione del dispositivo esistente, riconoscimento automatico della rete, configurazione e rimozione delle direttive di sicurezza.
SOFTNET Security Client service: Computer configuration	Lo stato attuale del sistema viene rilevato. I contenuti di questo file Log servono alla diagnostica dello stato del sistema se si verificano problemi. Il file Log supporta il servizio assistenza durante l'eliminazione del problema e contiene inoltre la configurazione del firewall, le impostazioni degli instradamenti e del sistema operativo del sistema nonché i programmi installati sul PC.
SOFTNET Security Client service: VPN Tunnel	Tutti i messaggi Log della Log console in the tunnel overview: Tempi di risposta in caso di risposta negativa a richieste ping, nome DNS risolto.
SOFTNET Security Client service: Reachability test	Controllo della raggiungibilità dei nodi interni e delle unità Security; tempi di risposta delle risposte positive e negative alle richieste ping.
SOFTNET Security Client GUI: General log file	Informazioni sull'avvio e la chiusura del SOFTNET Security Client. Il file Log contiene ad es. informazioni sull'avvio del SOFTNET Security Client, sul controllo della licenza e sul caricamento dei dati di configurazione.
SOFTNET Security Client: SCP	Compilazione del protocollo di dati del protocollo SCP. SCP viene utilizzato per trasmettere via tunnel informazioni sui nodi interni tra le unità Security interessate se i nodi interni non sono progettati in modo statico su queste unità Security.

8.10 Attivazione di regole firewall Windows - finestra di dialogo "Windows firewall parameter assignment"

Regola firewall Windows per il servizio SOFTNET Security Client

Selezionare nella finestra principale del SOFTNET Security Client la voce di menu "Settings" > "Windows firewall parameter assignment".

In questa finestra di dialogo è possibile attivare una regola firewall Windows per il servizio SOFTNET Security Client. Questa regola firewall Windows consente al servizio SOFTNET Security Client di ricevere pacchetti SCP in ingresso. Il protocollo SCP viene utilizzato per trasmettere via tunnel informazioni sui nodi interni delle unità Security tra queste unità Security se i nodi interni non sono progettati in modo statico su queste unità Security.

Nota

Osservare le "Avvertenze Security" e le avvertenze sulla parametrizzazione del firewall

Il SOFTNET Security Client può fornire un supporto solo limitato durante la parametrizzazione del firewall Windows in relazione al funzionamento sicuro di impianti, soluzioni, macchine, dispositivo e/o reti.

Osservare le "Avvertenze Security" e le avvertenze relative alla parametrizzazione del firewall nel manuale di progettazione e nella guida in linea del SOFTNET Security Client.

Le funzioni possibili sono riportate nella seguente tabella.

Funzione	Descrizione / Opzioni
Parametri della regola firewall	
Name, program (SOFTNET_Security_Client_Service.exe), description	Informazioni descritte relative alla regola firewall SOFTNET Security Client
Partner IP address, partner port, local IP address, local port, direction, protocol type	Vengono visualizzati in grigio i parametri impostati della regola firewall SOFTNET Security Client per protocollo e porte. Se si vogliono modificare questi parametri è possibile eseguire le modifiche tramite il pulsante "Advanced Windows Firewall".

Funzione	Descrizione / Opzioni
Profile and interface type	Indicare i profili e i tipi di interfaccia per i quali deve valere la regola firewall SOFTNET Security Client.
Global Windows firewall status	Profili firewall Windows Tramite il pulsante "Windows Firewall Profiles" è possibile inserire o disinserire il firewall Windows del sistema. Se è stata attivata la regola firewall Windows del SOFTNET Security Client, il firewall Windows deve essere inserito per la rispettiva rete: l'impostazione firewall Windows deve essere "attiva". Firewall Windows avanzato Con il pulsante "Advanced Windows Firewall" si accede alle regole in ingresso del firewall Windows con sicurezza avanzata. Se è stata attivata la regola firewall Windows del SOFTNET Security Client, le proprietà della regola possono essere modificate alla regola in ingresso.

Interazione del SOFTNET Security Client con il software del firewall di terzi.

In linea di principio è possibile l'utilizzo del SOFTNET Security Client insieme al software del firewall di terzi. Per consentire o bloccare le funzioni del SOFTNET Security Client è necessario tenere in considerazione i seguenti parametri nel software del firewall:

Protocollo	Porta locale	Porta dispositivo opposto	Direzione	Funzione	Commento
UDP	tutti	500	in uscita	IKE / IPSec	Negoziazione del tunnel VPN IKE/IPSec.
UDP	tutti	4500	in uscita	IKE / IPSec	Negoziazione del tunnel VPN IKE/IPSec. Necessario se sulla linea del tunnel VPN si trova almeno un dispositivo NAT
UDP	tutti	53	in uscita	DNS	Risoluzione del nome dell'unità DNS negli indirizzi IP.
ESP	*non appropriato*	*non appropriato*	su entrambi i lati	IPSec	Traffico di dati utili del tunnel VPN
UDP	tutti	3820	in ingresso	SCP	Istruzione automatica di nodi interni dei dispositivi VPN
ICMP	*non appropriato*	*non appropriato*	su entrambi i lati	Test di raggiungibilità	Pacchetti ICMP del controllo della raggiungibilità del SOFTNET Security Client.

8.11 Impostazioni SOFTNET Security Client - finestra di dialogo "Settings"

Impostazione per il SOFTNET Security Client

Selezionare nella finestra principale del SOFTNET Security Client la voce di menu "Settings" > "SOFTNET Security Client settings".

In questa finestra di dialogo effettuare le impostazioni che devono essere mantenute dopo la chiusura e l'apertura del SOFTNET Security Client.

Le funzioni possibili sono riportate nella seguente tabella.

Funzione	Descrizione / Opzioni
Log console in the tunnel overview	
I seguenti messaggi Log vengono visualizzati nella consolle Log della panoramica dei tunnel: • Negative reachability test (ICMP) • Creation/deletion of main modes (phase 1) • Creation/deletion of quick modes (phase 2) • Download configuration files • Learn internal nodes	Selezione dei tipi di messaggi che vengono visualizzati nella consolle Log della panoramica dei tunnel.
Number of displayed messages	Numero di messaggi che vengono estratti dai file Log e visualizzati nella consolle Log della panoramica dei tunnel.
Log files	
File size	Dimensione del rispettivo file Log che viene visualizzata in "Diagnostics" > "Log files" per messaggi di eventi rilevanti del sistema. Poiché i dati Log vengono salvati nel file tramite il buffer circolare, selezionare tramite la dimensione del file per quanto tempo i dati Log restano salvati nel file.
Message category	Messaggi di eventi rilevanti del sistema. Vengono visualizzati i messaggi relativi ad avvertimenti, errori di sistema e informazioni.
Open directory	
• Service log files • GUI log files	In entrambe queste directory vengono salvati tutti i file Log. I file Log del GUI SOFTNET Security Client vengono memorizzati separatamente dai file Log del servizio SOFTNET Security Client.
Language	
Program language	Selezione delle impostazione della lingua dell'interfaccia software (GUI). Le lingue selezionabili sono tedesco e inglese. Se la lingua è stata modificata è necessario un riavvio del SOFTNET Security Client.

Funzione	Descrizione / Opzioni
SCP learning functionality	
Learn internal nodes	Se nella configurazione delle unità Security è attivata la modalità di apprendimento, essa può essere utilizzata anche nel SOFTNET Security Client. In questo modo si ottengono automaticamente le informazioni sui nodi interni dinamici delle unità Security. Nella casella di visualizzazione sotto la casella di controllo viene visualizzato se il rispettivo firewall SSC è attivo. Esso può essere adattato tramite il pulsante "Change".
Show tunnel overview automatically in the foreground if an internal node changes	In caso di attivazione di questa funzione: Se è stato riconosciuto un nuovo nodo interno viene visualizzata la finestra di dialogo "Tunnel Overview".
Global reachability test	
• Enabled • Disabled	Se si disattiva questa funzione, viene disattivato il test di raggiungibilità globale per tutte le configurazioni contenute nel SOFTNET Security Client. Nella panoramica dei tunnel il test di raggiungibilità disattivato viene simboleggiato da un cerchio grigio. Vantaggio della disattivazione: La disattivazione ha il vantaggio che nessun pacchetto supplementare generi volumi di dati. Svantaggio della disattivazione: Nella panoramica dei tunnel non si riceve più nessun messaggio di risposta sul fatto che un nodo partner sia raggiungibile o meno.
Waiting time for response	Tempo di attesa impostabile per il ping che deve indicare la raggiungibilità di un partner del tunnel. **Avvertenza** Nei collegamenti via tunnel su percorsi di trasmissione lenti (reti di telefonia mobile: UMTS, GPRS) selezionare un tempo di attesa di ≥ 1500 ms. In questi percorsi di trasmissione il tempo di esecuzione dei pacchetti di dati è notevolmente aumentata. Il "tempo di attesa della risposta" influisce quindi direttamente la visualizzazione della raggiungibilità nella panoramica dei tunnel.

Funzione	Descrizione / Opzioni
Run time of the VPN tunnel	
• Permanent • Limited	**Utilizzo permanente dei tunnel VPN** I tunnel VPN vengono attivati quando l'utente esegue il login nel sistema operativo. In caso di disattivazione del sistema operativo i tunnel VPN vengono disattivati. **Utilizzo temporale limitato dei tunnel VPN** I tunnel VPN possono essere attivi solo nel tempo di esecuzione dell'interfaccia utente del SOFTNET Security Client. Chiudendo l'interfaccia utente vengono interrotti i tunnel VPN esistenti.

Funzioni online - Diagnostica e logging

9

Per scopi di test e di sorveglianza l'unità Security dispone di funzioni di diagnostica e di logging.

- Funzioni di diagnostica

  Sono intese diverse funzioni di sistema e di stato che possono essere utilizzate nella modalità online.

- Funzioni di logging

  Si tratta della registrazione degli eventi di sistema e di sicurezza.

La registrazione degli eventi viene eseguita nelle aree di buffer dell'unità Security o su un server Syslog. La parametrizzazione e l'analisi di queste funzioni presuppone un collegamento di rete sull'unità Security selezionata.

Registrazione di eventi con funzioni Logging

Gli eventi che devono essere registrati si definiscono con le impostazioni Log per la relativa unità Security.

Per la registrazione è possibile configurare le seguenti varianti:

- Logging locale

  In questa variante si registrano gli eventi nel buffer locale dell'unità Security. Nella finestra di dialogo Online del Security Configuration Tool è possibile quindi accedere a queste registrazioni, visualizzarle o archiviarle nella stazione di service.

- Syslog rete

  Con Network Syslog si utilizza un server Syslog esistente nella rete al quale vengono inviati eventi. Indicare nelle impostazioni Log della rispettiva unità Security gli eventi che vengono inviati.

Archiviazione di dati Log e lettura dal file

Per l'archiviazione gli eventi registrati possono essere salvati in un file Log che può essere aperto in modalità offline. A tal fine selezionare la voce di menu "Opzioni" > "File Log..." e selezionare tramite il pulsante "Apri..." il file Log da aprire. Ulteriori informazioni si trovano nel seguente capitolo:

- Panoramica delle funzioni della finestra di dialogo online (Pagina 251)

Diagnostica in modalità Ghost S602 ≥V3.1

Dopo il rilevamento di un indirizzo IP da un nodo interno l'unità Security sull'interfaccia esterna dispone di un indirizzo IP che può essere diverso dall'indirizzo IP con il quale l'unità Security è stata inizialmente progettata. Prima di poter eseguire una diagnostica tramite l'interfaccia esterna, nel Security Configuration Tool per l'interfaccia esterna è necessario sostituire l'indirizzo IP inizialmente progettato con quello che l'unità Security ha rilevato dal nodo interno per il tempo di esecuzione.

Protezione dei file log esportati da accesso non autorizzato

Dai file di log esportati dal Security Configuration Tool è possibile ottenere informazioni rilevanti per la sicurezza. Per questo motivo assicurarsi che i file siano protetti da accesso non autorizzato. Questo va osservato in particolare in caso di inoltro dei file.

9.1 Panoramica delle funzioni della finestra di dialogo online

L'unità Security offre le seguenti funzioni nella finestra di dialogo online del Security Configuration Tool:

Tabella 9- 1 Funzioni e logging nella diagnostica online

Funzione / scheda nella finestra di dialogo online		**Significato**
Funzioni di sistema e di stato		
	Status	Visualizzazione dello stato dei dispositivi nell'unità Security selezionata nel progetto.
SCA. S	Date and time	Impostazione di data e ora
S≥V3.0	Impostazioni dell'interfaccia	Panoramica delle impostazioni delle singole interfacce.
S≥V3.0	DNS dinamico	Panoramica delle impostazioni per il DNS dinamico
S≥V3.0	Tabella ARP	Visualizzazione della tabella ARP dell'unità Security.
S≥V3.0	Utenti connessi	Visualizzazione degli utenti che sono connessi alla pagina Internet per i set di regole IP specifici per l'utente.
~~S602~~	Stato della comunicazione	Visualizzazione dello stato di comunicazione e dei nodi interni delle unità Security che si trovano nello stesso gruppo VPN dell'unità Security selezionata.
~~S602~~ ~~PS CP~~	Nodi interni	Visualizzazione dei nodi interni dell'unità Security.
S7-CP	Regole firewall aggiornate dinamicamente	Visualizzazione degli indirizzi IP abilitati dinamicamente tramite HTTP o HTTPS oppure caricati successivamente da un utente. Un aggiornamento degli indirizzi IP in questa scheda può essere eseguito con i seguenti eventi: • Estensione/aggiornamento dell'elenco IP Access Control • Aggiornamento delle regole firewall • Estensioni dinamiche inserite dal CP durante l'esecuzione, ad es. PROFINET IO Device Poiché in questa scheda vengono visualizzate solo le regole firmware dinamiche aggiornate, nella visione completa dello stato attuale del firmware dell'unità devono essere incluse anche le regole firewall progettate offline.
S602 ≥V3.1	Modalità Ghost	Finestra di dialogo per la modalità Ghost di SCALANCE S602 con informazioni relative all'indirizzo IP del nodo interno (identico all'indirizzo IP esterno dell'unità Security) e al cambio di indirizzo IP sul nodo interno.
S≥V4.0	Blacklist IP	Visualizzazione degli indirizzi IP che sono stati inseriti nella Blacklist del firewall.

Funzione / scheda nella finestra di dialogo online		Significato
Funzioni di logging		
	System Log	Visualizzazione degli eventi di sistema logging nonché avvio e arresto della visualizzazione.
	Audit Log	Visualizzazione degli eventi di sicurezza logging nonché avvio e arresto della visualizzazione.
	Log filtro pacchetto	Visualizzazione dei pacchetti di dati logging nonché avvio e arresto della visualizzazione.

Informazioni più dettagliate sulle possibilità di impostazione nelle singole schede si trovano nella guida in linea.

Requisiti per l'accesso

Per poter utilizzare le funzione online su un'unità Security devono essere soddisfatti i seguenti requisiti:

- è in atto un collegamento di rete con l'unità selezionata
- il progetto, con il quale è stata configurata l'unità, è aperto
- il modo di funzionamento online nel Security Configuration Tool è attivo o la diagnostica online specifica per l'unità è stata aperta tramite il menu di scelta rapida.
- Per i CP deve essere abilitato l'accesso per la diagnostica nel firewall (TCP 443)

Nota

Presupposto per la diagnostica online in modalità Ghost S602 ≥V3.1

La diagnostica online è disponibile in modalità Ghost solo quando l'unità Security ha appreso l'indirizzo IP del nodo interno e ha acquisito la sua interfaccia esterna. Successivamente l'unità Security è raggiungibile tramite l'indirizzo IP dell'interfaccia esterna.

Messaggio di avvertimento in caso di configurazione non attuale o di un altro progetto

Se si richiama la finestra di dialogo online si controlla se la configurazione attuale sull'unità Security e la configurazione del progetto caricato corrispondono. Se le configurazioni sono diverse, viene visualizzato un messaggio di avvertimento. In questo modo viene segnalato che la configurazione non è (ancora) stata aggiornata o che si utilizza il progetto errato.

Visualizzazione dello stato di registrazione

Lo stato attuale di registrazione risulta dalla configurazione caricata o dalla configurazione modificata nella finestra di dialogo online. Le impostazioni buffer possibili sono memoria circolare o memoria lineare. L'impostazione attualmente attiva può essere rilevata nel modo seguente:

1. Passare al modo di funzionamento con la voce di menu "Visualizza" > "Online" .
2. Selezionare l'unità Security da modificare.
3. Selezionare la voce di menu "Modifica" > "Diagnostica online...".

   Non appena si apre una delle schede per le funzioni Log, nella parte inferiore della scheda si vede lo stato attuale dell'impostazione buffer dell'unità Security selezionata:

Le impostazioni online non vengono memorizzate nella configurazione

Le impostazioni che si eseguono nel modo di funzionamento online (ad es. impostazioni buffer nelle funzioni Log) non vengono salvate nella configurazione sull'unità Security. Per questo motivo dopo un nuovo avvio dell'unità diventano sempre attive le impostazioni della configurazione offline.

9.2 Registrazione di eventi (logging)

Informazioni generali

Gli eventi sull'unità Security possono essere registrati. La registrazione viene eseguita nelle aree del buffer volatili o permanenti, a seconda del tipo di evento. In alternativa una registrazione può essere eseguita in un server di rete.

Configurazione in modalità standard e in modalità estesa

Le possibilità di selezione nel Security Configuration Tool dipendono dalla visualizzazione selezionata:

- Modalità standard

  In modalità standard il "Logging locale" è attivato come standard; gli eventi del filtro pacchetto possono essere attivati globalmente nella scheda "Firewall". In questa visualizzazione non è possibile il "Network Syslog".

- Modalità estesa

  Tutte le funzioni di logging possono essere attivate o disattivate nella scheda "Impostazioni Log" di un'unità; gli eventi del filtro pacchetto devono inoltre essere attivati in modo selettivo nella scheda "Firewall" (regole locali o globali).

Metodi di registrazione e classi di evento

Nella configurazione è possibile definire i dati che devono essere registrati. In questo modo la registrazione si attiva già durante il caricamento della configurazione nell'unità Security.

Inoltre selezionare nella configurazione uno o entrambi i metodi di registrazione possibili:

- Logging locale
- Network Syslog

L'unità Security conosce i seguenti eventi per entrambi i metodi di registrazione:

Funzionamento	Tipo di funzione
Eventi pacchetto filtro (firewall)	Il Log filtro pacchetto registra determinati pacchetti del traffico di dati. Vengono registrati solo pacchetti di dati interessati da una regola filtro pacchetto progettata (firewall) o sui quali reagisce la protezione di base (pacchetti corrotti o non validi). Come presupposto la registrazione per la regola del filtro pacchetto deve essere attivata.
Eventi Audit	L'Audit Log registra automaticamente in modo sequenziale gli eventi rilevanti per la sicurezza, quali ad es. le azioni dell'utente come l'inserimento e il disinserimento del logging pacchetto.
Eventi di sistema	Il Log di sistema registra automaticamente gli eventi progressivi, quali ad es., l'avvio di un processo o le azioni per le quali un utente non si è autenticato correttamente tramite password. La registrazione è scalabile in base alle classi di evento.
	Diagnostica della linea: Inoltre è progettabile una diagnostica del cavo. La diagnostica del cavo fornisce messaggi non appena il numero di pacchetti di telegramma errati ha superato il valore limite impostabile.

Metodo di memorizzazione per la registrazione dei dati nel logging locale

La memorizzazione per la registrazione dei dati viene eseguita in base a due metodi selezionabili:

- Memoria circolare

Al raggiungimento della fine del buffer la registrazione all'inizio del buffer viene proseguita sovrascrivendo le voci meno recenti.

- Memoria lineare

La registrazione di arresta quando il buffer è pieno.

Attivazione e disattivazione del logging

In modalità estesa, con le impostazioni Log nel modo di funzionamento "Offline" è possibile attivare il logging locale per le classi di evento nelle proprietà dell'unità e definire il metodo di memorizzazione. Queste impostazioni Log vengono caricate nell'unità con la configurazione e attivate all'avvio dell'unità Security.

In caso di necessità, nelle funzioni online è possibile attivare o disattivare il logging locale per gli eventi del filtro pacchetto e gli eventi di sistema. Durante questa operazione le impostazioni nella configurazione del progetto non vengono modificate.

Visualizzazione dello stato di registrazione

Le impostazioni online non vengono memorizzate nella configurazione.

9.2.1 Logging locale - Impostazioni nella configurazione

Con le impostazioni Log, nel modo di funzionamento "Offline" è possibile attivare le classi di evento e definire il metodo di memorizzazione. Queste impostazioni Log vengono caricate nell'unità con la configurazione e attivate all'avvio dell'unità Security.

In caso di necessità, le impostazioni Log progettate possono essere modificate nelle funzioni online. Durante questa operazione le impostazioni nella configurazione del progetto non vengono modificate.

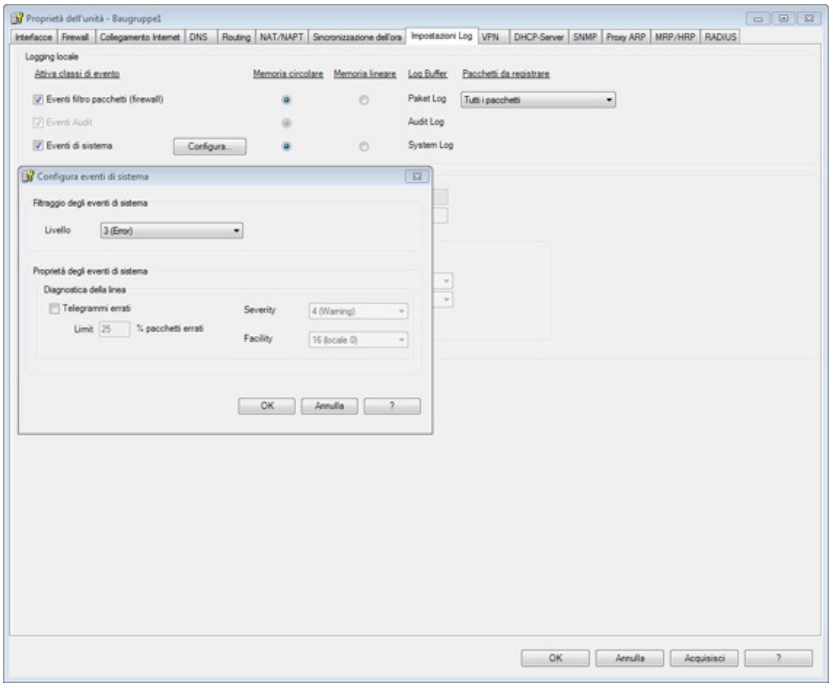
Impostazioni Log nella modalità standard

Le impostazioni Log nella modalità standard corrispondono alle preimpostazioni della modalità estesa. Nella modalità standard Mode non è tuttavia possibile modificare le impostazioni.

Impostazioni Log nella modalità estesa

1. Selezionare l'unità da modificare.
2. selezionare la voce di menu "Modifica " > Proprietà...", scheda "Impostazioni Log"

La seguente finestra di dialogo illustra le impostazioni standard per l'unità Security; inoltre è aperta la finestra di dialogo per la configurazione della registrazione degli eventi di sistema:



Configurazione delle classi di evento

Tabella 9- 2 Log locale - Panoramica delle funzioni

Funzione / scheda nella finestra di dialogo online	Progettazione	Osservazioni
Eventi pacchetto filtro (firewall)	L'attivazione avviene tramite casella opzionale. La selezione del metodo di memorizzazione avviene tramite campi opzione. Dalla casella di riepilogo "Pacchetti registrati" è possibile stabilire la quantità di pacchetti di dati registrati: • "Tutti i pacchetti": Vengono registrati pacchetti di dati interessati da una regola firewall progettata (modalità standard o modalità estesa). Inoltre vengono registrati i pacchetti di risposta ai pacchetti che hanno attraversato il firewall in base alla regola Allow progettata. • "Pacchetti che generano lo stato": Vengono registrati solo i pacchetti di dati interessati da una regola firewall progettata (modalità standard o modalità estesa).	I dati Log del filtro pacchetto non sono ritentivi I dati vengono depositati in una memoria volatile dell'unità Security, per questo motivo essi non sono più disponibili dopo un disinserimento della tensione di alimentazione.
Eventi Audit (sempre attivati)	Il Logging è sempre attivato. La memorizzazione avviene sempre nel buffer circolare.	I dati Log Audit sono ritentivi I dati vengono depositati in una memoria ritentiva dell'unità Security, per questo motivo essi sono ancora disponibili dopo un disinserimento della tensione di alimentazione. **Avvertenza per CP:** I dati Audit Log non sono ritentivi nei CP. Per la sicurezza dei dati è quindi necessario utilizzare un server Syslog.
Eventi di sistema	L'attivazione avviene tramite casella opzionale. La selezione del metodo di memorizzazione avviene tramite campi opzione. Per la configurazione del filtro evento e della diagnostica del cavo aprire un'altra finestra di dialogo con il pulsante "Configure...".	I dati Log di sistema non sono ritentivi I dati vengono depositati in una memoria volatile dell'unità Security, per questo motivo essi non sono più disponibili dopo un disinserimento della tensione di alimentazione.

Funzione / scheda nella finestra di dialogo online	Progettazione	Osservazioni
Filtraggio degli eventi di sistema	Impostare in questa sotto-finestra di dialogo un livello di filtro per gli eventi di sistema. Come standard sono impostati i seguenti valori: • SCALANCE S: Livello 3 • CP: Livello 3	Selezionare come livello del filtro "Error" o un valore superiore per escludere la registrazione di eventi generali non critici. **Avvertenza per il CP** Selezionare per il CP solo il livello 3 o il livello 6. • In caso di selezione del livello 3 vengono visualizzati i messaggio di errore dei livelli da 0 a 3. • In caso di selezione del livello 6 vengono visualizzati i messaggio di errore dei livelli da 0 a 6.
Diagnostica della linea	La diagnostica del cavo crea un evento di sistema specifico. Impostare a partire da quale percentuale di telegrammi errati deve essere generato un evento di sistema. Assegnare una Facility o una Severity all'evento di sistema.	Con la Severity si valutano gli eventi di sistema della diagnostica della linea in relazione alla Severity degli altri eventi di sistema. **Avvertenza** Non assegnare agli eventi di sistema della diagnostica della linea nessuna Severity inferiore al filtraggio dell'evento di sistema. In caso contrario questi eventi non vengono filtrati e registrati.

9.2.2 Network Syslog - Impostazioni nella configurazione

L'unità Security può essere configurata come client che invia informazioni Logging ad un server Syslog. Il server Syslog può trovarsi in una sotto-locale rete interna o esterna. L'implementazione corrisponde a RFC 3164.

Nota

Firewall - Syslog Server non attivo nella rete esterna

Se il Syslog Server non è attivo sul computer indirizzato, questo computer restituisce telegrammi di risposta ICMP "port not reachable". Se a causa della configurazione firewall questi telegrammi di risposta vengono registrati come eventi di sistema e inviati al server Syslog, questa operazione può proseguire all'infinito (valanga di eventi).

Rimedi:

- Avviare il Syslog server;
- Modificare le regole del firewall;
- Togliere dalla rete il computer con il server Syslog disattivato.

Eseguire le impostazioni Log

1. Commutare il modo di funzionamento con la voce di menu "Visualizza" > "Modalità estesa" .

Nota

Non è possibile una ricommutazione alla modalità standard

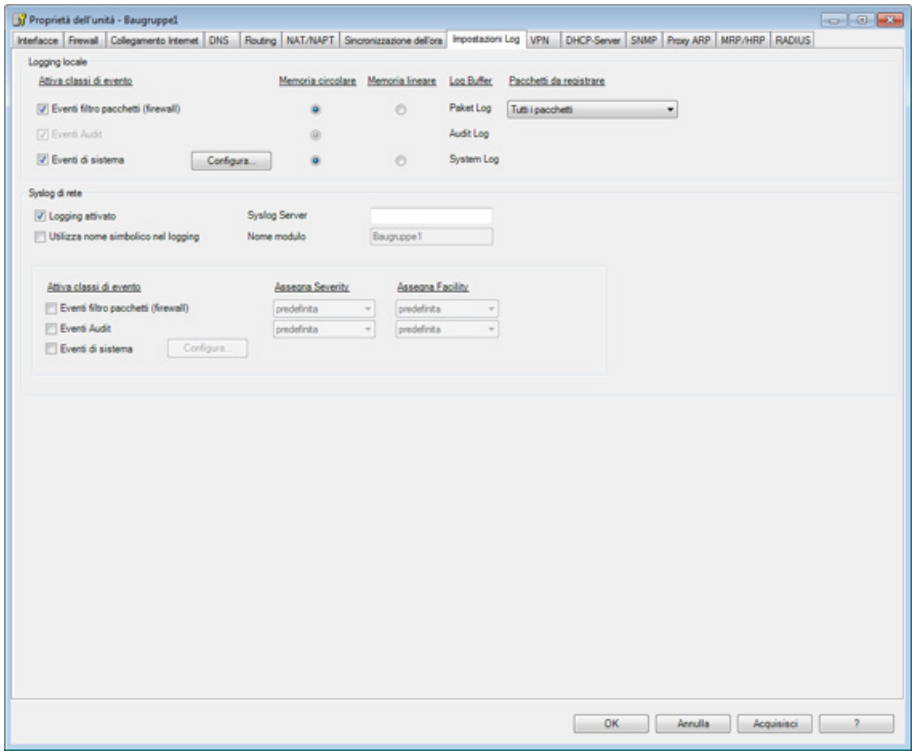
Non appena è stata modificata la configurazione per il progetto attuale, non è più possibile annullare una commutazione nella modalità estesa precedentemente eseguita.

Rimedio SCT Standalone: chiudere il progetto senza salvarlo e aprirlo di nuovo.

---

2. Selezionare l'unità Security da modificare.
3. selezionare la voce di menu "Modifica " > Proprietà...", scheda "Impostazioni Log"

La seguente finestra di dialogo illustra le impostazioni standard per l'unità Security con Logging attivato per la rete Syslog:



Realizzazione del collegamento al server Syslog

Per SCALANCE S: L'unità Security utilizza il nome di unità progettato come nome host rispetto al server Syslog.

Per CP: L'unità Security utilizza il proprio indirizzo IP come nome host rispetto al server Syslog.

Inserire nella casella "Server Syslog" l'indirizzo IP / il FQDN del server Syslog. L'indirizzo IP può essere inserito in alternativa come nome simbolico o numerico.

L'unità Security deve poter accedere al server Syslog tramite l'indirizzo IP indicato o eventualmente tramite la progettazione del router nella scheda "Routing". Se il server Syslog non viene raggiunto, l'invio delle informazioni Syslog viene disattivata. Questo stato operativo può essere riconosciuto dai relativi messaggi del sistema. Per riattivare l'invio delle informazioni Syslog è eventualmente necessario aggiornare le informazioni di routing e riavviare il modulo Security.

Utilizzo del nome simbolico nel Logging

Attivare la casella opzione "Utilizza nome simbolico nel Logging", le indicazioni di indirizzo dei telegrammi Log trasmesse al server Syslog vengono sostituite con nomi simbolici. L'unità Security verifica la progettazione dei relativi nomi simbolici e li inserisce nei telegrammi Log.

Nota

Maggiore tempo di elaborazione in caso di nomi simbolici

Se la casella opzione "Utilizza nomi simbolici nel Logging" è attivata, il tempo di elaborazione nell'unità Security viene aumentato.

Per gli indirizzi IP dell'unità Security vengono utilizzati automaticamente i nomi delle unità come nomi simbolici. Nella modalità Routing questi nomi vengono ampliati con una sigla di porta nel modo seguente: "Nome unità-P1", "Nome unità-P2" ecc.

Configurazione delle classi di evento

Tabella 9- 3 Network Syslog - Panoramica delle funzioni

Funzione / scheda nella finestra di dialogo online	Progettazione	Osservazioni
Eventi pacchetto filtro (firewall)	L'attivazione avviene tramite la casella opzione. Mediante l'impostazione di Facility e Severity i messaggi Syslog possono essere classificati in merito alla loro provenienza e alla loro gravità. L'assegnazione avviene tramite casella di riepilogo. A ciascun evento viene assegnata la Severity e la Facility, qui impostata.	Il valore da selezionare dipende dall'analisi nel server Syslog. Questo consente un adattamento ai requisiti nel server Syslog. Se si lascia impostato il valore standard "default", con l'unità Security si definisce la combinazione di Facility e Severity con la quale viene visualizzato l'evento.
Eventi Audit	L'attivazione avviene tramite la casella opzione. L'assegnazione della Severity e Facility avviene tramite le caselle di riepilogo. A ciascun evento viene assegnata la Severity e la Facility, qui impostata.	Il valore da selezionare per la Severity e la Facility dipende dall'analisi nel server Syslog. Questo consente un adattamento ai requisiti nel server Syslog. Se si lascia impostato il valore standard "default", con l'unità Security si definisce la combinazione di Facility e Severity con la quale viene visualizzato l'evento.

Funzione / scheda nella finestra di dialogo online	Progettazione	Osservazioni
Eventi di sistema	L'attivazione avviene tramite la casella opzione.	Per la configurazione del filtro evento e della diagnostica del cavo aprire un'altra finestra di dialogo con il pulsante "Configure...".
Filtraggio degli eventi di sistema	Impostare in questa sotto-finestra di dialogo un livello di filtro per gli eventi di sistema. Come standard sono impostati i seguenti valori: • SCALANCE S: Livello 3 • CP: Livello 3	Selezionare come livello del filtro "Error" o un valore superiore per escludere la registrazione di eventi generali non critici. **Avvertenza per il CP** Selezionare per il CP solo il livello 3 o il livello 6. • In caso di selezione del livello 3 vengono visualizzati i messaggio di errore dei livelli da 0 a 3. • In caso di selezione del livello 6 vengono visualizzati i messaggio di errore dei livelli da 0 a 6.
Diagnostica della linea	La diagnostica del cavo crea un evento di sistema specifico. Impostare a partire da quale percentuale di telegrammi errati deve essere generato un evento di sistema. Assegnare una Facility o una Severity all'evento di sistema.	Con la Severity si valutano gli eventi di sistema della diagnostica della linea in relazione alla Severity degli altri eventi di sistema. **Avvertenza** Non assegnare agli eventi di sistema della diagnostica della linea nessuna Severity inferiore al filtraggio dell'evento di sistema. In caso contrario questi eventi non vengono filtrati e registrati dal server Syslog.

9.2.3 Progettazione del logging pacchetti

Progettazione del logging in modalità standard

Le informazioni relative al logging di set di regole IP e MAC si trovano nei seguenti capitoli:

- SCALANCE S in modalità standard (Pagina 124)
- CP in modalità standard (Pagina 113)

Nota

CP

Correlazione tra le impostazioni Log in modalità standard e regole firewall

Le impostazioni Log in modalità standard non hanno effetto per le regole firewall che sono state create automaticamente con una progettazione del collegamento. In questo modo non è possibile eseguire ad es. il logging di telegrammi via tunnel di un collegamento progettato. In modalità estesa il logging alle regole firewall generate automaticamente può essere estesa a ulteriori collegamenti.

Progettazione del logging in modalità estesa

L'attivazione del logging è identica per entrambi i tipi di regole (IP o MAC) e tutte le regole. Per registrare i pacchetti di dati di determinate regole del filtro pacchetti, impostare nella colonna "Logging" della scheda "Firewall" un segno di spunta.

Appendice

A

A.1 Conformità DNS

La conformità DNS secondo RFC1035 comprende le seguenti regole:

- limitazione a 255 caratteri complessivi (lettere, numeri, trattino o punto)
- il nome deve iniziare con una lettera alfabetica;
- il nome deve finire solo con una lettera alfabetica o con un numero;
- una componente del nome all'interno del nome, cioè una catena di caratteri tra due punti può essere lunga max. 63 caratteri;
- nessun carattere speciale come dieresi, parentesi, sottolineatura, barra, spazio vuoto ecc.

A.2 Aree dei valori indirizzo IP, maschera della sottorete indirizzo dell'accoppiamento ad altra rete

Area dei valori per indirizzo IP

L'indirizzo IP è composta da 4 numeri decimali dell'area di valori compresa tra 0 e 255, separati tra loro da un punto; ad es. 141.80.0.16

Area dei valori per maschera della sotto-rete

La maschera della sotto-rete è composta da 4 numeri decimali dell'area di valori compresa tra 0 e 255, separati tra loro da un punto, ad es. 255.255.0.0

I 4 numeri decimali della maschera della sotto-rete devono contenere nella rappresentazione binaria da sinistra una sequenza di valori senza spazi "1" e da destra una sequenza di valori senza spazi "0".

I valori "1" determinano il numero di rete all'interno dell'indirizzo IP. I valori "0" determinano l'indirizzo Host all'interno dell'indirizzo IP.

Esempio:

Valori corretti:

255.255.0.0 decimale = 11111111.11111111.00000000.00000000 binario

255.255.128.0 decimale = 11111111.11111111.10000000.00000000 binario

255.254.0.0 decimale = 11111111.11111110.00000000.00000000 binario

Valore errato:

255.255.1.0 decimale = 11111111.11111111.00000001.00000000 binario

Relazione tra indirizzo IP e maschera della sotto-rete

Il primo numero decimale dell'indirizzo IP (da sinistra) determina la struttura della maschera della sotto-rete riguardo al numero dei valori "1" (binari) nel modo seguente (per "x" sta l'indirizzo Host):

Primo numero decimale dell'indirizzo IP	Finestra della sotto-rete
0 ... 127	255.x.x.x
128 ... 191	255.255.x.x
192 ... 223	255.255.255.x

Nota:

Per il primo numero decimale dell'indirizzo IP è possibile inserire anche un valore compreso tra 224 e 255. Tuttavia questo non è raccomandabile in quanto questa area di indirizzi è riservata per altri compiti e in alcuni tool di configurazione (ad es. STEP 7) per questi valori non viene eseguito nessun controllo.

Area dei valori per indirizzo dell'accoppiamento ad altra rete

L'indirizzo è composto da 4 numeri decimali dell'area di valori compresa tra 0 e 255, separati tra loro da un punto; ad es. 141.80.0.1.

Relazione indirizzo IP e indirizzo dell'accoppiamento ad altra rete

L'indirizzo IP e l'indirizzo dell'accoppiamento ad altra rete devono essere diversi solo nelle posizioni nelle quali è riportato "0" nella maschera della sotto-rete.

Esempio:

È stato inserito: per la maschera della sotto-rete 255.255.255.0; per l'indirizzo IP 141.30.0.5 e per l'indirizzo dell'accoppiamento ad altra rete 141.30.128.254. L'indirizzo IP e l'indirizzo dell'accoppiamento ad altra rete possono presentare un valore diverso solo nel 4° numero decimale. Nell'esempio è tuttavia già diversa la terza posizione.

Nell'esempio deve quindi essere modificato in alternativa:

la maschera della sotto-rete a: 255.255.0.0 o

l'indirizzo IP a: 141.30.128.5 o

l'indirizzo dell'accoppiamento ad altra rete a: 141.30.0.254

A.3 MAC adress

Avvertenza relativa alla struttura dell'indirizzo MAC:

Gli indirizzi MAC sono indirizzi hardware per l'identificazione di nodi di rete. Un indirizzo MAC è costituito da sei byte che vengono annotati in modo esadecimale separati da trattini.

L'indirizzo MAC è composto da una parte fissa e una parte variabile. La parte fissa ("Indirizzo di base MAC") indica il produttore (Siemens, 3COM, ...). La parte variabile dell'indirizzo MAC distingue i diversi nodi Ethernet.

Adattamento della MTU (Maximum Transmission Unit)

La MTU definisce la grandezza massima dei pacchetti di dati trasmissibili attraverso la rete. Quando vengono trasmessi da SCALANCE S attraverso il tunnel IPsec, i pacchetti di dati aumentano di dimensioni perché vi vengono aggiunte le informazioni dell'intestazione; in alcuni casi devono essere quindi segmentati per poter essere trasmessi interamente. Questo dipende dalle specifiche MTU della rete collegata. La segmentazione può tuttavia compromettere notevolmente le prestazioni della rete o persino causare l'interruzione della trasmissione dei dati.

Per evitare questi problemi si deve adattare, ovvero ridurre, il formato MTU, in modo che i pacchetti di dati ricevuti da SCALANCE S possano essere integrati con le necessarie informazioni aggiuntive senza che sia in seguito necessario segmentarli. È consigliabile impostare una dimensione compresa tra 1000 e 1400 byte.

Bibliografia

B

B.1 Introduzione - senza CD/DVD

Come trovare la documentazione SIMATIC NET

- **Cataloghi**

  I numeri di ordinazione per i prodotti Siemens qui rilevanti si trovano nei seguenti cataloghi:

  – SIMATIC NET Comunicazione industriale / identificazione industriale, Catalogo IK PI

  – SIMATIC Prodotti per Totally Integrated Automation e Micro Automation, Catalogo ST 70

  I cataloghi nonché informazioni supplementari possono essere richiesti presso la consulenza Siemens locale.

  Industry Mall si trova in Internet al seguente indirizzo:

  Link a Siemens Industry Mall (http://www.siemens.com/industrymall)

- **Documentazione in Internet**

  I manuali SIMATIC NET si trovano anche nelle pagine Internet del Siemens Automation Customer Support:

  Link al Customer Support (http://support.automation.siemens.com/WW/view/it)

  Navigare al gruppo di prodotti desiderato ed eseguire le seguenti impostazioni:

  Scheda "Elenco articoli", Tipo di articolo "Manuali / Manuali operativi"

- **Documentazione nell'installazione di STEP 7**

  Ai manuali presenti nella documentazione online dell'installazione di STEP 7 sul PG/PC, si accede tramite il menu di avvio ("Start" > "Tutti i programmi" > "Siemens Automation" > "Documentazione").

Vedere anche

Link alla documentazione:
(http://www.automation.siemens.com/simatic/portal/html_00/techdoku.htm)

B.2 CP S7 / Per la progettazione, la messa in servizio e l'utilizzo del CP

/1/

SIMATIC NET
CO S7 per Industrial Ethernet
Progettazione e messa in servizio
Manuale parte A - Applicazioni generali
Manuale di progettazione
Siemens AG
(SIMATIC NET Manual Collection)
In Internet alla seguente ID articolo:
30374198 (http://support.automation.siemens.com/WW/view/it/30374198)

/2/

SIMATIC NET

CP S7 per Industrial Ethernet

Manuale parte B

Manuale

Siemens AG

(SIMATIC NET Manual Collection)

In Internet si trovano i manuali per i singoli CP alla seguente ID articolo:

CP 343-1 Advanced (GX31): 28017299
(http://support.automation.siemens.com/WW/view/it/28017299)

CP 443-1 Advanced (GX30): 59187252
(http://support.automation.siemens.com/WW/view/it/59187252)

B.3 Per la progettazione con STEP 7 / NCM S7

/3/

SIMATIC NET
NCM S7 per Industrial Ethernet
Prontuario di esempi applicativi
Siemens AG
(parte integrante della documentazione online in STEP 7)

/4/

SIMATIC NET
Messa in servizio di stazioni PC - Istruzioni e guida rapida
Manuale di progettazione
Siemens AG
(SIMATIC NET Manual Collection)
In Internet alla seguente ID articolo:
13542666 (http://support.automation.siemens.com/WW/view/it/13542666)

/5/

SIMATIC
Configurazione hardware e progettazione di collegamenti con STEP 7
Siemens AG
(parte del pacchetto di documentazione "Nozioni di base STEP 7")
(parte integrante della documentazione online in STEP 7)

B.4 CP S7 Per il montaggio e la messa in servizio del CP

/6/

SIMATIC S7
Sistema di automazione S7-300

- Configurazione della CPU 31xC e 31x: Istruzioni operative
  ID articolo: 13008499 (http://support.automation.siemens.com/WW/view/it/13008499)
- Dati dell'unità: Manuale di riferimento
  ID articolo: 8859629 (http://support.automation.siemens.com/WW/view/it/8859629)

Siemens AG

e

SIMATIC S7
sistema di automazione S7-400, M7-400

- Configurazione Manuale di installazione
  ID articolo: 1117849 (http://support.automation.siemens.com/WW/view/it/1117849)
- Dati dell'unità: Manuale di riferimento
  ID articolo: 1117740 (http://support.automation.siemens.com/WW/view/it/1117740)

Siemens AG

B.5 Per la configurazione e il funzionamento di una rete Industrial Ethernet

/7/

SIMATIC NET
Manuale reti Twisted Pair e Fiber Optic
Siemens AG
(SIMATIC NET Manual Collection)

B.6 Nozioni di base SIMATIC e STEP 7

/8/

SIMATIC
Comunicazione con SIMATIC
Manuale di sistema
Siemens AG
ID articolo:
25074283 (http://support.automation.siemens.com/WW/view/it/25074283)

/9/

Pacchetto di documentazione "Nozioni fondamentali STEP 7"

- Primi passi ed esercitazioni con STEP 7 (ID: 18652511 (http://support.automation.siemens.com/WW/view/it/18652511))
- Programmazione con STEP 7 (ID: 18652056 (http://support.automation.siemens.com/WW/view/it/18652056))
- Configurazione hardware e progettazione di collegamenti con STEP 7 (ID: 18652631 (http://support.automation.siemens.com/WW/view/it/18652631))
- Manuale di conversione da S5 a S7 (ID: 1118413 (http://support.automation.siemens.com/WW/view/it/1118413))

Siemens AG
Numero di ordinazione 6ES7 810-4CA08-8AW0

(Componente della documentazione Online in STEP 7)

B.7 Comunicazione industriale volume 2

/10/

SIMATIC NET
Industrial Ethernet Manuale di rete
Siemens AG

(SIMATIC NET Manual Collection)

In Internet alla seguente ID articolo: 27069465
(http://support.automation.siemens.com/WW/view/it/27069465)

B.8 Per la configurazione di stazioni PC / PG

/11/

SIMATIC NET
Messa in servizio delle stazioni PC - Manuale e guida rapida
Manuale di progettazione
Siemens AG
ID articolo: 13542666 (http://support.automation.siemens.com/WW/view/it/13542666)

B.9 Per la configurazione CP PC

/12/

SIMATIC NET Industrial Ethernet CP 1628

Manuale operativo compatto
Siemens AG

(SIMATIC NET Manual Collection)

In Internet alla seguente ID articolo: 56714413
(http://support.automation.siemens.com/WW/view/it/56714413)

B.10 SIMATIC NET Industrial Ethernet Security

/13/

SIMATIC NET Industrial Ethernet Security
SCALANCE S a partire da V3.0

Manuale di installazione e messa in servizio
Siemens AG

(SIMATIC NET Manual Collection)

In Internet alla seguente ID articolo: 56576669
(http://support.automation.siemens.com/WW/view/it/56576669)

/14/

SIMATIC NET Industrial Remote Communication
SCALANCE M-800

Manuale di progettazione
Siemens AG

(SIMATIC NET Manual Collection)

In Internet alla seguente ID articolo: 78389151

Vedere anche

78389151 (http://support.automation.siemens.com/WW/view/it/78389151)

/15/

SIMATIC NET
Telecontrol SCALANCE M875

Manuale operativo
Siemens AG

(SIMATIC NET Manual Collection)

In Internet alla seguente ID articolo: 58122394
(http://support.automation.siemens.com/WW/view/it/58122394)

Indice analitico

*

*.cer, 211, 231
*.dat, 231
*.p12, 84, 211, 231

3

3DES, 201

A

Accordo di chiave Diffie-Hellman, 201
Account ISP, 98
Advanced Encryption Standard (AES), 201
AES, 189, 201
Aggiornamento del firmware, 72
Amministratore, 67
Applet, 71
Area dei valori per indirizzo IP, 263
Area del contenuto, 88
ARP, 193
ARP Proxy, 190
Assegnazioni ai gruppi, 57
Attivazione della comunicazione via tunnel
    CP x43-1 Adv., 113
    SCALANCE S < V3.0, 132
    SCALANCE S V3, 129
Attivazione firewall
    CP 1628, 113
    CP x43-1 Adv., 113
    SCALANCE S < V3.0, 132
    SCALANCE S V3, 129
Authentification, 65
Autocrossing, 96
Autonegotiation, 96
Autorità di certificazione, 81, 82
Autorizzazioni utente, 70

B

Banda indirizzo, 151
Blacklist IP, 251
Broadcast, 167
Buffer, 254

C

Certificate Authority, 80
Certificati FTPS, 80
Certificato, 81, 194
    autofirmato, 83
    Esportazione, 80
    firmato da un'autorità di certificazione, 83
    Importazione, 80
    rinnovo, 82
    sostituzione, 84, 84
Certificato CA, 80, 83, 84
Certificato del gruppo CA, 84
Certificato SSL, 83
CHAP, 98
Check Consistency, 104, 183
    in tutto il progetto, 61
    locale, 61
Codifica, 43, 60
Collegamenti non specificati, 53
Collegamenti specificati, 53, 111
Collegamento di rete, 236
Comando PING, 237
Comunicazione IP
    con protocollo S7, 132
    dalla rete interna a quella esterna, 132
Configurazione della gestione dell'ora, 186
Conformità DNS, 263
Controllo della coerenza, 63
CP 1628
    Funzione, 38
CP PC, 3
CP S7, 3
CP x43-1 Adv.
    Funzione, 36
C-PLUG, 40, 60
Creazione dell'instradamento, 164

D

Data Encryption Standard (DES), 202
Dati di configurazione
    lettura, 234
DCP, 133
DCP (Primary Setup Tool), 159
Dead-Peer-Detection (DPD), 206

DES, 189, 202
DHCP
Configurazione server, 180
Server, 132
Symbolic Names, 62
Diagnostica, 249
Diagnostica della linea, 254, 257, 260
Diagnostica online, 253
Dipendenze dal diritto, 71
Diritti dell'apparecchio, 70
Diritti di progettazione, 70
Dispositivo VPN, 86
Certificato unità, 214
DNS
Server, 133
Durata dei certificati, 199
Durata massima della sessione, 66, 68
Durata SA, 202
DVD del prodotto SCALANCE S, 44

E

Elenco IP Access Control, 71
Esporta server NTP, 188
Eventi Audit, 254
Eventi di sistema, 254
Eventi filtro pacchetto, 254

F

Facility, 259
Filtro pacchetto IP
locale, 144
Finestra della sotto-rete, 88
Finestra di dialogo principale, 233
Firewall, 29
Modalità estesa, 134
Regole firewall, 111
Symbolic Names, 62
FTP, 71
FTP/FTPS, 54
Fullduplex, 93
Funzionalità tunnel, 191
Funzionamento VLAN, 194

G

Gestione utenti, 57, 64
Glossario, 7
Glossario SIMATIC NET, 7
Gruppo di servizi, 160
Gruppo VPN, 198

H

Halfduplex, 93
HTTP, 152

I

ICMP, 144
ID rete, 164
IEEE 802.3, 29, 111
IKE, 114, 120
Impostazioni
in tutto il progetto, 57
Impostazioni IKE, 200
Impostazioni IPsec, 200
Impostazioni Security, 229
Indirizzo dell'accoppiamento ad altra rete, 264
Indirizzo Gigabit, 83
Indirizzo IP, 150, 263
Indirizzo IP router, 165
Indirizzo IP WAN
definizione, 207
Indirizzo PROFINET, 83
Informazioni sullo stato, 238
Installazione
SCALANCE S, 43
Interfacce, 163
Internet Key Exchange (IKE), 201
ISAKMP, 207

L

Larghezza di banda, 147, 156
Layer 2, 111, 134, 193
Layer 3, 111, 134
Layer 4, 111
LLDP, 71
Logging, 112, 249
Classi di evento, 259
CP x43-1 Adv., 113
SCALANCE S < V3.0, 132
SCALANCE S V3, 129
Logging locale, 249, 254, 256
Eventi Audit, 256
Eventi di sistema, 256
Eventi filtro pacchetto, 256

M

M-800, 3, 212
MAC adress, 264
Manager dei certificati, 81
Maschera della sottorete, 263
MD5, 189, 202
Memoria circolare, 254
Memoria lineare, 254
Metodo di autenticazione, 194, 200
MIB, 71
Modalità Aggressive, 201
modalità bridge, 94
Modalità di programmazione, 219
Modalità estesa, 42
  Logging, 261
  Logging locale, 253, 255
  Network Syslog, 253
  Regole firewall, 134
  Regole firewall globali, 135
  Regole firewall specifiche per l'utente, 138
  Server DHCP, 181
Modalità Ghost, 94
Modalità Main, 201
Modalità Routing, 94, 163
  attivazione, 163
Modalità standard, 42
  Firewall, 112
  Logging, 260
  Logging locale, 253
Multicast, 167

N

NAT/NAPT
  Routing, 165
NCP VPN Client, 86
  Certificato del gruppo, 215
  Certificato del gruppo CA, 215
  Creazione del file di configurazione, 213, 215
Network Syslog, 254
Nodi attivi, 203
Nodi con indirizzo IP sconosciuto, 204
Nodi di rete esterni
  CP x43-1 Adv., 38
  SCALANCE 602, 27
  SCALANCE S612 / S623 / S627-2M, 30
Nodi di rete interni
  Configurazione, 217
  CP x43-1 Adv., 38
  SCALANCE 602, 27
  SCALANCE S612 / S623 / S627-2M, 30
Nome ruoli, 68
Nome simbolico, 62, 259
Nome utente, 66
Nomi del gruppo, 152, 158
NTP
  Symbolic Names, 62, 62
NTP (secure), 186
NTP Server, 133, 186

P

Panoramica delle funzioni
  Tipi di unità, 18
PAP, 98
Parametri di indirizzo, 88
Password, 235
Perfect Forward Secrecy, 202
Porta
  102 (protocollo S7 - TCP), 152
  123 (NTP), 167
  20/21 (FTP), 152
  443 (HTTPS), 167, 167
  4500 (IPsec), 167
  500 (IPsec), 167
  500 (ISAKMP), 207
  514 (Syslog), 167
  80 (HTTP), 152
Preimpostazione firewall
  CP 1628, 119
  CP x43 Adv., 114
  SCALANCE S < V3.0, 124
Preshared Keys, 194
Prodotto di un altro produttore, 86
PROFINET, 219
Progetto
  Valori di inizializzazione, 60
Proprietà configurabili, 233
Proprietà del gruppo, 200
Proprietà del gruppo VPN, 200
Proprietà dell'unità, 85
Protezione contro l'accesso, 40
Protezione di accesso IP, 54
Protocollo, 152
Protocollo ESP, 114, 120, 202
Protocollo IP, 134
Protocollo ISO, 219
Protocollo MAC, 134

R

Regole del filtro pacchetto IP, 145
CP 1628, 148
CP x43-1 Adv., 148
SCALANCE S, 148
Regole del filtro pacchetto MAC, 154, 155
Regole firewall automatiche, 141
Regole firewall globali, 135
assegnazione, 137
Regole firewall locali, 112, 135
Regole firewall predefinite
CP x43-1 Adv., 113, 113
SCALANCE S < V3.0, 132
SCALANCE S V3, 129
Regole firewall specifiche per l'utente, 138
Parametro timeout, 141
Utente accesso remoto, 67
Regole pacchetto filtro globali, 137
Regole per il collegamento, 142
Rete piatta, 94
Riconoscimento di nodi, 237
Rinnovo del certificato del gruppo CA, 203
Router NAT/NAPT
Nome simbolico, 62
Router standard, 88, 164
Routing interfacce, 94
Routing interfaccia, 86
Ruoli, 67
definiti dal sistema, 67
definito dall'utente, 68
Ruoli definiti dall'utente, 68
Ruolo definito dal sistema
administrator, 67
diagnostics, 67
remote access, 67
standard, 67

S

SCALANCE M, 3
Autorità di certificazione, 211
Certificato del gruppo, 211
Creazione del file di configurazione, 210
SCALANCE M875, 3, 212
SCALANCE S, 3
Creazione dell'unità, 85
Sistemi operativi supportati, 43
SCALANCE S602
Funzione, 25
SCALANCE S612
Funzione, 28
SCALANCE S623
Funzione, 28
SCALANCE S627-2M
Funzione, 28
Schede di rete, 236
Security Configuration Tool, 40, 41, 42
in STEP 7, 42, 51
Installazione, 44
Installazione CP x34-1 Adv., 44
Installazione del CP 1628, 44
Modalità di comando, 42
Standalone, 42, 51
Senza retroeffetto, 30
Server DHCP, 182
Servizi ICMP, 153
Servizi IP, 152
Servizi MAC, 158
Set di regole firewall
definite dall'utente, 138
globali, 57
Set di regole firewall globali, 155
Set di regole IP, 135
specifici per l'utente, 138
Set di regole IP specifiche per l'utente, 139
Set di regole MAC, 135
Severity, 259
SHA1, 189, 202
SiClock, 159
Significato dei simboli, 5
Simboli, 5
Sincronizzazione dell'ora, 186
Sistemi operativi supportati
SCALANCE S, 43
SOFTNET Security Client, 229
SNMP, 71
SNMPv1, 189
SNMPv3, 189
SOFTNET Security Client, 3
Base dati, 231
Comportamento all'avvio, 230
configurazione nel progetto, 230
Creazione del file di configurazione, 230
disinstallazione, 230
Funzione, 24
Sistemi operativi supportati, 229
spionaggio dei dati, 28
Stateful Packet Inspection, 111
STEP 7, 51
Dati migrati, 52
Migrazione utenti, 64
Proprietà dell'oggetto, 52
Strutture d'insieme, 20

Syslog
Eventi Audit, 259
Eventi di sistema, 260
Eventi filtro pacchetto, 259
Symbolic Names, 62
Syslog server, 59, 249, 257
Syslog rete, 249

T

TCP, 144, 152
Telegrammi dell'ora SiClock, 133
Telegrammi Ethernet-Non-IP, 111
Telegrammi non-IP, 193
Tunnel, 191, 234
Collegamenti via tunnel, 235
Configurazione, 236
Tunnel IPsec, 191

U

UDP, 144, 152
Unità Security, 3
Unknown Peers, 204
Utente accesso remoto, 67
Utenti
Assegnazione dei ruoli, 69
configurazione, 66
Creazione dei ruoli, 67
Non privilegiati, 239
Privilegiati, 239
Utenti di diagnostica, 67
Utenti non privilegiati, 239
Utenti privilegiati, 239
Utenti standard, 67

V

Valori di inizializzazione standard, 60
Versione del firmware, 4
Visualizzazione di diagnostica online, 42
Visualizzazione di progettazione offline, 42
VLAN tagging, 194
VPN, 24, 191
Proprietà specifiche per l'unità, 205
SOFTNET Security Client, 227